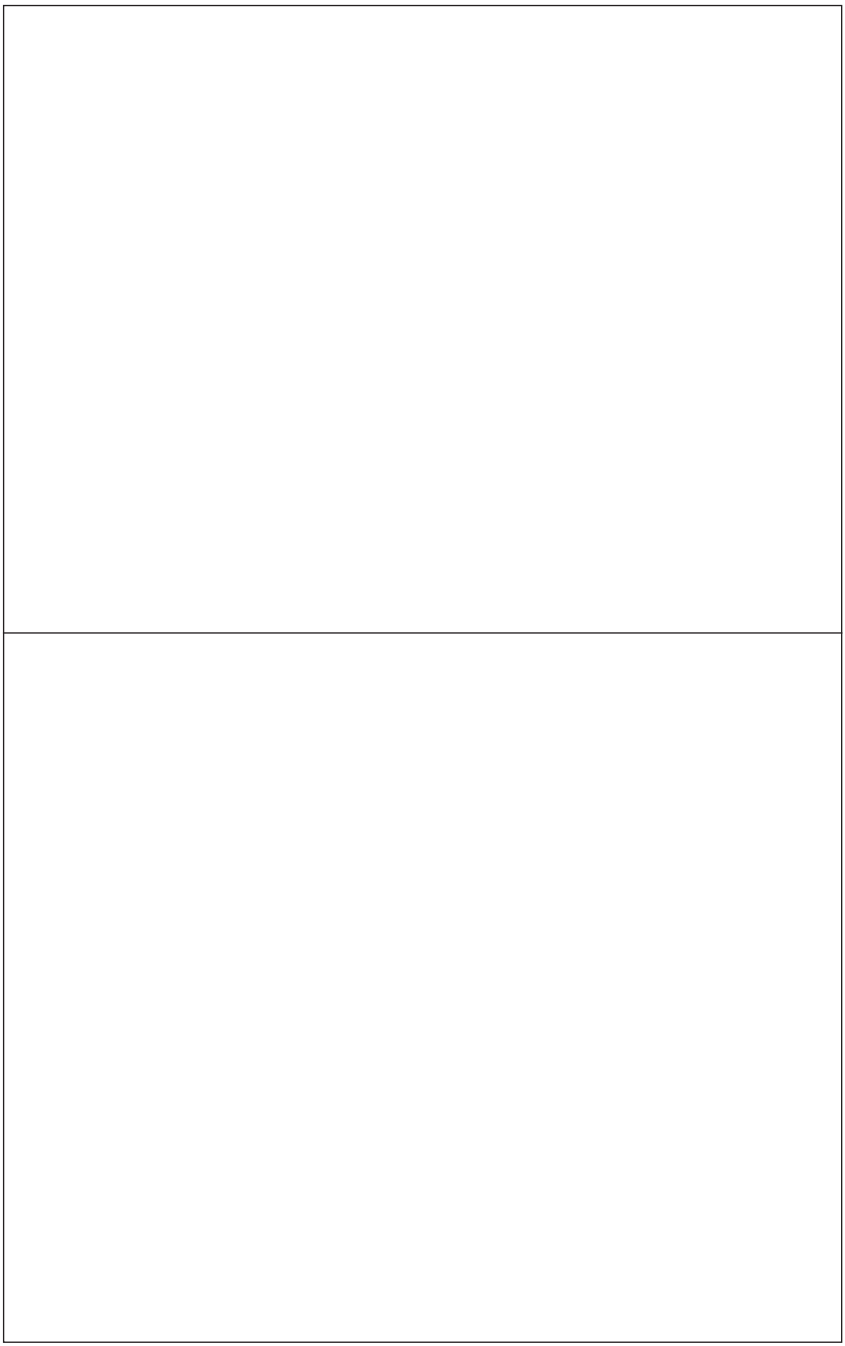
Sohyun Park

Der Schutz personenbezogener Daten im Strafverfahren

Eine rechtsvergleichende Untersuchung zum deutschen und US-amerikanischen Recht

Nomos



Sohyun Park

Der Schutz personenbezogener Daten im Strafverfahren

Eine rechtsvergleichende Untersuchung zum deutschen und US-amerikanischen Recht

Nomos

The book processing charge was funded by the Baden-Württemberg Ministry of Science, Research and Arts in the funding programme Open Access Publishing and the University of Freiburg.

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Zugl.: Freiburg, Univ., Diss., 2021

1. Auflage 2021

Publiziert von
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden
www.nomos.de

Gesamtherstellung:
Nomos Verlagsgesellschaft mbH & Co. KG
Waldseestraße 3–5 | 76530 Baden-Baden

ISBN (Print): 978-3-8487-8379-3
ISBN (ePDF): 978-3-7489-2769-3

DOI: https://doi.org/10.5771/9783748927693

Onlineversion
Nomos eLibrary

Vorwort

Die vorliegende Arbeit wurde im Wintersemester 2020/2021 von der juristischen Fakultät der Albert-Ludwigs-Universität Freiburg als Dissertation angenommen. Rechtsprechung und Schrifttum wurden bis Mitte Oktober 2020 ausgewertet.

Bezüglich des Abschlusses meiner Promotion danke ich vor allem meinem Doktorvater, Herrn Prof. Dr. Ulrich Sieber, für seine hervorragende Unterstützung bei der Betreuung dieser Arbeit und für seine große Hilfe bei der Veröffentlichung. Dank seiner konstruktiven Kommentare und Anregungen im Rahmen der Research School am Max-Planck-Institut für ausländisches und internationales Strafrecht in Freiburg im Breisgau gelang es mir, die Dissertation fertigzustellen. Außerdem bedanke ich mich bei Herrn Prof. Dr. Hans-Jörg Albrecht für die Erstellung des Zweitgutachtens. Für die Hilfe bei der Veröffentlichung möchte ich den freundlichen Mitarbeiterinnen und Mitarbeitern des Nomos-Verlags sowie vor allem Herrn Prof. Dr. Johannes Rux danken.

Besonderen Dank schulde ich meinem koreanischen Betreuer, Herrn Prof. Dr. Seongdon Kim von der Sungkyunkwan-Universität. Er hat mir nicht nur den Weg für das Studium in Deutschland geebnet, sondern mir auch die Ausrichtung für mein gesamtes Studium gegeben und mir die nötigen wissenschaftlichen Grundlagen vermittelt.

Ich möchte mich auch bei meinen Freunden bedanken, die bei mir waren und dank derer das Leben im Ausland für mich nicht einsam und insofern weniger schwierig war. Mein Dank gilt darüber hinaus auch den Mitgliedern der Arbeitsgruppe, mit denen ich in Deutschland studiert habe.

Ohne die Unterstützung meiner Eltern wäre diese Arbeit nicht zustande gekommen. Ich danke ihnen von ganzem Herzen dafür, dass sie immer an meiner Seite geblieben und mich sowohl finanziell unterstützt als auch seelisch ermutigt haben. Dank ihnen konnte ich mein Studium in Deutschland abschließen und meine Dissertation veröffentlichen. Insbesondere möchte ich auch meiner älteren Schwester Jeeyoun Park Danke sagen, die immer wie meine engste Freundin bei mir steht. Ich danke Gott für seine Gnade. Meinen Eltern widme ich diese Arbeit.

Uiwang, 15. Juni 2021 *Sohyun Park*

Inhaltsverzeichnis

Verzeichnis der Tabellen und Schaubilder

Abkürzungsverzeichnis

a. a. O.	am angegebenen Ort
ABl.	Amtsblatt
Abs.	Absatz
AEUV	Vertrag über die Arbeitsweise der Europäischen Union
a. F.	alte Fassung
AO	Abgabenordnung
Art.	Artikel
Aufl.	Auflage
BAnz	Bundesanzeiger
Bd.	Band
BDSG	Bundesdatenschutzgesetz
BeckOK-StPO	Beck'scher Onlinekommentar zur StPO
BfJ	Bundesamt für Justiz
BGBl.	Bundesgesetzblatt
BGH	Bundesgerichtshof
BGHSt	Entscheidungen des Bundesgerichtshofs in Strafsachen
BKA	Bundeskriminalamt
BKAG	Gesetz über das Bundeskriminalamt und die Zusammenarbeit des Bundes und der Länder in kriminalpolizeilichen Angelegenheiten
BMJ	Bundesministerium für Justiz
BT-Drs.	Drucksachen des Deutschen Bundestages
BVerfGE	Entscheidungen des Bundesverfassungsgerichts
BVerfGG	Gesetz über das Bundesverfassungsgericht
BVerfSchG	Gesetz über die Zusammenarbeit des Bundes und der Länder in Angelegenheiten des Verfassungsschutzes und über das Bundesamt für Verfassungsschutz
BZR	Bundeszentralregister
BZRG	Gesetz über das Zentralregister und das Erziehungsregister
BZRGVwV	Allgemeine Verwaltungsvorschrift zur Durchführung des Bundeszentralregistergesetzes

bzw.	beziehungsweise
CALEA	Communications Assistance for Law Enforcement Act
CDU/CSU	Christlich Demokratische Union Deutschlands/ Christlich-Soziale Union in Bayern
C.F.R.	Code of Federal Regulations
CR	Computer und Recht
ders.	derselbe
DEA	Drug Enforcement Administration
d. h.	das heißt
DOJ	U.S. Department of Justice
DSGVO	Datenschutzgrundverordnung
DuD	Datenschutz und Datensicherheit
ECPA	Electronic Communications Privacy Act
EDV	Elektronische Datenverarbeitung
EGV	Vertrag zur Gründung der Europäischen Gemeinschaft
EMRK	Europäische Menschenrechtskonvention
EU	Europäische Union
EuGH	Gerichtshof der Europäischen Union
FAG	Gesetz über Fernmeldeanlagen
FBI	Federal Bureau of Investigation
f./ff.	folgende/fortfolgende
FIRS	Fingerprint Identification Records System
FISA	Foreign Intelligence Surveillance Act
FISC	Foreign Intelligence Surveillance Court
FISCR	Foreign Intelligence Surveillance Court of Review
Fn.	Fußnote
FOIA	Freedom of Information Act
FTC	Fair Trade Commission
GA	Goltdammer‘s Archiv für Strafrecht
GG	Grundgesetz
GRC	Charta der Grundrechte der Europäischen Union

GVG	Gerichtsverfassungsgesetz
HK-stopp	Heidelberger Kommentar zur Strafprozessordnung
Hrsg.	Herausgeber
HStR	Handbuch des Staatsrechts
ICT	Information and Communications Technology
III-System / Triple I-System	Interstate Identification Index
IMEI	International Mobile Equipment Identity
IMSI	International Mobile Subscriber Identity
i. S. d.	im Sinne des
ISP	Internet Service Provider
IT	Informationstechnologie
i. V. m.	in Verbindung mit
i. w. S.	im weiten Sinne
JGG	Jugendgerichtsgesetz
Jura	Juristische Ausbildung
JuS	Juristische Schulung
JVEG	Gesetz über die Vergütung von Sachverständigen, Dolmetscherinnen, Dolmetschern, Übersetzerinnen und Übersetzern sowie die Entschädigung von ehrenamtlichen Richterinnen, ehrenamtlichen Richtern, Zeuginnen, Zeugen und Dritten
KMR	KMR-Kommentar zur Strafprozessordnung
KK-StPO	Karlsruher Kommentar zur Strafprozessordnung
KriPoZ	Kriminalpolitische Zeitschrift
lit.	Litera
LR-StPO	Löwe-Rosenberg, Die Strafprozessordnung und das Gerichtsverfassungsgesetz: Großkommentar
MNI	Master-Name-Index
m. w. N.	mit weiteren Nachweisen
NASA	National Aeronautics and Space Administration
NCIC	National Criminal Information Center

NFF	National Fingerprint File
n. F.	neue Fassung
NICS	National Instant Criminal Background Check System
NJ	Neue Justiz
NJW	Neue Juristische Wochenschrift
NLETS	National Law Enforcement Telecommunications System
Nr.	Nummer
NRW	Nordrhein-Westfalen
NSA	National Security Agency
NStZ	Neue Zeitschrift für Strafrecht
NVwZ	Neue Zeitschrift für Verwaltungsrecht
o. Ä./o. ä.	oder Ähnliche(s)/oder ähnlich
OECD	Organization for Economic Co-operation and Development
OLG	Oberlandesgericht
OrgKG	Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der organisierten Kriminalität
OVG	Oberverwaltungsgericht
RAV	Republikanischer Anwältinnen- und Anwälteverein e. V.
RGBl.	Reichsgesetzblatt
RL	Richtlinie
Rn.	Randnummer
S.	Seite(n)
SCA	Stored Communications Act
SK-StPO	Systematischer Kommentar zur Strafprozessordnung und Gerichtsverfassungsgesetz
sog.	sogenannt
SPD	Sozialdemokratische Partei Deutschlands
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
StV	Strafverteidiger
StVÄG	Strafverfahrensänderungsgesetz
TDDSG	Teledienstdatenschutzgesetz

TDSV	TELEKOM-Datenschutzverordnung
TK	Telekommunikation
TKG	Telekommunikationsgesetz
u. a.	und andere/unter anderem
URL	Uniform Resource Locator
USA	United States of America
USAF	USA Freedom Act
U.S.C.	Code of Laws of the United States of America
usw.	und so weiter
v.	von
vs.	versus
VG	Verwaltungsgericht
vgl.	vergleiche
VoZählG	Gesetz über eine Volks-, Berufs-, Gebäude-, Wohnungs- und Arbeitsstättenzählung
z. B.	Zum Beispiel
ZRP	Zeitschrift für Rechtspolitik
ZStV	Zentrales Staatsanwaltschaftliches Verfahrensregister
ZStVBetrV	Verordnung über den Betrieb des Zentralen Staatsanwaltschaftlichen Verfahrensregisters
ZStW	Zeitschrift für die gesamte Strafrechtswissenschaft

Einleitung

A. Freiheit und Sicherheit im digitalen Zeitalter

I. Daten als Machtquelle

Im digitalen Zeitalter sind Informationen[1] Macht. Die Erhebung, Speicherung und Nutzung von Daten ist zu einer wichtigen Ressource für den gesamten sozialen und wirtschaftlichen Austausch geworden. Die Macht der Information offenbart sich vor allem dann, wenn im Zuge moderner Datenverarbeitungsprozesse, bei denen in Echtzeit Daten in riesigen Mengen erzeugt werden, ein im Grunde unbedeutendes Datenelement durch die der Informationstechnologie inhärenten Verarbeitungs- und Verknüpfungsmöglichkeiten einen neuen Stellenwert erhält. Die mit dem Aufkommen des digitalen Zeitalters einhergehenden Veränderungen in unserem Leben brachten unter anderem die Entwicklung und die rasche Verbreitung des Personal Computers (PC) mit sich. Durch die Entwicklung von Datenbanken und der jeweils zugehörigen Office-Software-Typen wurden Arbeitsprozesse in erheblichem Maße beschleunigt und erleichtert. Anders als bei der Verwendung von Papier, das einem physischen Verfallsprozess unterliegt, können Daten beliebig lange gespeichert und abgerufen werden. Einmal gespeichertes Wissen geht nicht mehr verloren und ist jederzeit zugänglich. Die Entwicklung des World Wide Web hat die rapide Steigerung der Erzeugung, der Verteilung und des Verbrauchs von Daten verursacht. Die hochgradig entwickelte Informationstechnologie hat folglich das Leben des Einzelnen auf signifikante Weise verändert. Des Weiteren ist das technische Verständnis im Umgang mit dem Computer für die

1 Laut *Luciano Floridi* werden vier Arten von miteinander kompatiblen Phänomenen als Information bezeichnet: 1) Informationen über etwas (z. B. einen Zugfahrplan); 2) Informationen als etwas (z. B. DNA oder Fingerabdrücke); 3) Informationen für etwas (z. B. Algorithmen oder Anweisungen); 4) Informationen in etwas (z. B. ein Muster oder eine Beschränkung). Nach *Floridi* wird das Wort „Informationen" meist metaphorisch oder abstrakt verwendet, was dazu führt, dass dessen Bedeutung unklar ist. Hier bezieht sich das Wort „Information" jedoch auf Erkenntnisse, die durch die Kombination und die Analyse verschiedener Daten erhalten wurden. Es wird also verwendet, um Informationen von Daten als solchen zu unterscheiden.

Bürger zu einem entscheidenden Faktor geworden, um als Mitglied auf dem neu strukturierten Arbeitsmarkt bestehen zu können.[2]

Die Entwicklung der elektronischen Kommunikationstechnologie, die Universalisierung des Internets und die Verbreitung des PC haben es Einzelpersonen ermöglicht, zeit- und ortsunabhängig Zugang zu Daten zu haben, verschiedene Daten zu sammeln sowie neue Daten zu schaffen und zu verarbeiten. Unter dem Schlagwort *Informationsgesellschaft* leben die Bürger im 21. Jahrhundert, fernab des industriell geprägten Lebens vorangehender Generationen, in einer neu geschaffenen, digitalen Welt des zeit- und ortsunabhängigen Zugangs zu Informationen, der Kommunikation via E-Mail sowie der Möglichkeit des elektronischen Geschäftsverkehrs.[3] Man kann mit einer kleinen und leichten Kreditkarte, einem Computer oder einem Smartphone wirtschaftliche Transaktionen durchführen, verschiedene Daten sammeln oder neue Daten erzeugen und verarbeiten. Durch Kreditkartentransaktionen anstelle von Barzahlungen wird die Transaktionshistorie schnell an Kreditkartenunternehmen, Produkthersteller sowie Informationsunternehmen übertragen. Diese Unternehmen sammeln und verarbeiten die übermittelten Daten, um sie zum Zwecke der Gestaltung ihrer Werbung oder ihrer Produkte anzuwenden. Die Besuche der Webseiten über das Internet hinterlassen Cookies auf dem Computer des Benutzers. Diese Cookies werden von Unternehmen ebenfalls zur Sammlung von Daten für die Analyse des Verbraucherverhaltens genutzt. So können personenbezogene Daten, die über das Internet übertragen werden, auf verschiedene Weise verwendet werden. Auch durch die Verwendung zunächst unbedeutend scheinender Datenelemente können aufgrund des Umstands, dass große Mengen an Daten elektronisch gesammelt, verarbeitet und genutzt werden, durch die Kombination mit unzähligen weiteren Daten neue Informationen generiert werden. Veränderungen in der sozialen Struktur führen zu Veränderungen in der Lebensweise und Denkweise der Menschen. In einer solchen Gesellschaft kann niemand leugnen, dass die Fähigkeit, Daten zu sammeln, zu verarbeiten und zu nutzen, eine wesentliche Rolle spielt. Heutzutage ist das

2 *Weidner-Braun*, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung – am Beispiel des personenbezogenen Datenverkehrs im www nach deutschem öffentlichen Recht, S. 26 m. w. N.

3 *Weidner-Braun*, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung – am Beispiel des personenbezogenen Datenverkehrs im www nach deutschem öffentlichen Recht, S. 17 m. w. N.

menschliche Leben ohne die Informationstechnologie nicht mehr vorstellbar.

II. Daten als neue Bedrohungsquelle der Freiheit

Es ist offensichtlich, dass die Verbreitung des Internets, die automatisierte Datenverarbeitung, die verbesserten Zugangsmöglichkeiten zu Daten und das World Wide Web das Alltagsleben der Menschen bequemer gestalten. Neben diesen Vorteilen entstehen jedoch auch viele Nachteile oder zumindest Umstände, bezüglich derer man Bedenken anmelden kann. Diese Bedenken betreffen vor allem die mögliche Beeinträchtigung der Grundrechte der Bürger und die potenzielle Entwicklung von einem Verfassungs- zu einem Überwachungsstaat. Die elektronische Verarbeitung personenbezogener Daten macht es Einzelpersonen schwer oder unmöglich, ihre Daten zu kontrollieren. Unter den Bedingungen der modernen Datenverarbeitung stellen die Bürger ihre personenbezogenen Daten oft zur Verfügung, ohne zu wissen, wo und wie ihre Daten verwendet und wohin sie übermittelt werden. Die Erweiterung der Speicherung sowie die uneingeschränkte Verarbeitung personenbezogener Daten ermöglichen es Unternehmen, Medien und sogar dem Staat, tiefere Einblicke in das Privatleben von Einzelpersonen zu gewinnen, wodurch die Freiheitsrechte dieser Einzelpersonen potenziell gefährdet sind. Die Bürger müssten in so einem Fall die sogenannte *Zero Privacy Society*[4] fürchten, in der ihre personenbezogenen Daten nicht vor potenziellem Missbrauch durch Befugte oder Unbefugte sicher sind. Niemand könnte sich hier vor einem möglichen Missbrauch personenbezogener Daten, sei es durch den Staat, durch Privatpersonen und insbesondere durch Unternehmen, absichern. Werden Daten durch Computer und Netzwerke über das Internet verarbeitet und kontrolliert, kann die unbefugte Datenspeicherung sowie der unbefugte Zugriff auf oder die unbefugte Verwendung von gespeicherten Daten schwerwiegende Konsequenzen haben. Personenbezogene Daten, die durch Computer und das Internet erhalten werden, werden im privaten Sektor hauptsächlich

4 *Scott McNealy*, CEO von Sun Microsystems, sagte einmal: „Wir haben bereits ‚zero privacy'. Finden Sie sich damit ab." (*Solove/Rotenberg/Schwartz*, Information Privacy Law, S. 635); „It is already far too late to prevent the invasion of cameras and databases. The djinn cannot be crammed back into its bottle. No matter how many laws are passed, it will prove quite impossible to legislate away the new surveillance tools and databases" (*Brin*, The Transparent Society, S. 8–23).

zu dem Zweck gesammelt und verarbeitet, die Verbrauchsmuster von Käufern zu analysieren und die Arbeitshaltung am Arbeitsplatz zu verwalten. Beispielsweise bietet die *Ubiquitous-Technologie*[5] einen Mechanismus zur Weitergabe und Überwachung personenbezogener Daten, der weiter geht als je zuvor, da beim Herstellen einer Verbindung zu einem Endgerät über ein bestimmtes Netzwerk sowohl der aktuelle Standort des Benutzers als auch weitere nachverfolgbare Verhaltensmuster in Echtzeit angezeigt werden können.

III. Datennutzung im Strafverfahren

Auf staatlicher Ebene werden zum Schutz der öffentlichen Sicherheit internationale Antiterrornetzwerke aufgebaut. Hierbei werden beträchtliche Mengen personenbezogener Daten von Bürgern gesammelt und gespeichert. Diese Tendenz ist auch im Strafverfahren zu beobachten. Der Um-

---

5 Einhergehend mit dem Eintreten in die *Ubiquitous Society* werden vier Internet-Szenarien für die Zukunft vorgeschlagen: 1) eine Welt, in der die menschlichen Bedürfnisse in hohem Maße berücksichtigt werden; 2) eine Welt, in der die grundlegenden Leistungen für alle angeboten werden; 3) eine Welt, in der jeder Inhalt, jedes Gerät oder jedes Format jederzeit abrufbar sind und 4) eine Welt, in der Viren, Spam, Junkmails oder Hacking nicht existieren können (Digital Dystopia). (Smart Internet Technology CRC, „Smart Internet 2010“, 09.2005). Durch die Kombination von Informationstechnologien wird eine *Ubiquitous-Gesellschaft* geschaffen, die die Bedürfnisse von Einzelpersonen, Ländern oder Gesellschaften jederzeit und überall in Echtzeit befriedigen kann. Der Ausdruck *Ubiquitous-Technologie* bezieht sich dabei auf eine Technologie, die die Fernsteuerung von alltäglichen Bedarfsgegenständen, Haushaltsgeräten und automatisierten Wohnräumen über eine Vielzahl von alltäglichen Bedarfsgegenständen ermöglicht, die hochmoderne Mikro-Halbleiter enthalten und die jederzeit und überall den Zugriff auf ein großes Netzwerk ermöglichen. Dies erzeugt ein Umfeld, das verschiedene Informationskommunikationsdienste nutzen kann, indem es unabhängig von Zeit und Ort auf das Informationskommunikationsnetzwerk zugreift. Es handelt sich um eine Voraussetzung für die allgegenwärtige Netzwerktechnologie, die Computer- sowie Informations- und Kommunikationstechnologien in verschiedene Geräte und Objekte integriert, sodass die Benutzer jederzeit und überall miteinander kommunizieren können. Es geht also um eine Gesellschaft, deren Gebrauchsgegenstände „intelligent“ (smart) und miteinander vernetzt sind, um die Kommunikation zwischen Menschen und Menschen, zwischen Gegenständen und Menschen und sogar zwischen Gegenständen und Gegenständen zu ermöglichen. Des Weiteren wird die Wettbewerbsfähigkeit des Staates durch die Verbesserung der individuellen Lebensqualität, die Steigerung der Unternehmensproduktivität und die Innovation öffentlicher Dienstleistungen gestärkt.

gang mit personenbezogenen Daten, insbesondere mit denen, die elektronisch gespeichert sind, hat im Strafprozessrecht in den letzten Jahren eine immer größere Bedeutung erlangt. Im Zuge des technischen Fortschritts haben sich die strafprozessualen Ermittlungen geändert. Das Aufkommen von Computern, die große Mengen an Informationen speichern können, hat die Polizei dazu veranlasst, diese zu Zwecken von Rasterfahndungen zu nutzen.[6] Nach den Terroranschlägen vom 11. September 2001 führte die Angst vor neuen Terroranschlägen weltweit zu einer Diskussion um den Einsatz umfassender und effektiver Antiterrormaßnahmen.[7] Diese Angst führte zu einem erhöhten Bedürfnis nach Sicherheit und Prävention, das ihrerseits zur Schaffung neuer Straftatbestände und Ermittlungsmaßnahmen führte, auch auf Kosten der Freiheit. Auf dieser Grundlage entstanden in der jüngeren Vergangenheit und entstehen weiterhin in der Strafprozessordnung neuartige Ermittlungsmethoden, die elektronische personenbezogene Daten verwenden. Aufgrund der Verbreitung sozialer Netzwerke steht dabei ein bedeutender Datenschatz zur Verfügung, der auf vielfältige Art und Weise genutzt werden kann. Die Möglichkeiten zur Verbrechensaufklärung sind beispielsweise durch die Verfügbarkeit von Verkehrsdaten besser geworden. In dieser Hinsicht bietet die technische Entwicklung große Vorteile für strafprozessuale Ermittlungen.

Wo jedoch die Veröffentlichung von Informationen und der unkomplizierte Zugang zu personenbezogenen Daten allgegenwärtig ist, besteht die Gefahr, dass der Schutz der Persönlichkeit des Einzelnen und – in Verbindung damit – sein Recht auf Wahrung einer geschützten Privatsphäre zugunsten übergeordneter Interessen der Gemeinschaft in den Hintergrund treten. Für die Effektivität der Ermittlung (Sicherheitsgarantie) ist die möglichst umfangreiche Speicherung und Auswertung möglichst vieler Daten offensichtlich nützlich. Dabei werden die Sicherheitsinteressen des Staates nicht selten stärker gewichtet als die von diesen staatlichen Eingriffsbefugnissen betroffenen Freiheitsrechte der Bürger.[8] Dies kann

6 Ende der siebziger, Anfang der achtziger Jahre sorgten Veröffentlichungen in der Presse über durchgeführte Datenabgleiche für gesteigerte Aufmerksamkeit. So wurde bekannt, dass die Ermittlungsbehörden sich mehrfach und mit unterschiedlichem Erfolg der Rasterfahndung bedient hatten.

7 *Weidner-Braun*, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung – am Beispiel des personenbezogenen Datenverkehrs im www nach deutschem öffentlichen Recht, S. 18.

8 *Bundesbeauftragter für den Datenschutz,* 19. Tätigkeitsbericht – 2001–2002, BT-Drs. 15/888, S. 24 f.; *Weichert,* Grundrechte in der Informationsgesellschaft, DuD 2000, 104, 106; *Germann,* Gefahrenabwehr und Strafverfolgung im Internet, S. 35.

jedoch zu einer grenzüberschreitenden Überwachung durch den Staat führen. Denn es besteht die Möglichkeit, dass einzelne Datenbankkonstruktionen oder Personalisierungsarbeiten, die mit personenbezogenen Daten in öffentlichen und nichtöffentlichen Sektoren durchgeführt werden, durch die öffentliche Sicherheitsgarantie sowie die Aufrechterhaltung der Ordnung und des Gemeinwohls oder durch optimale Nutzung von personell und materiell begrenzten Ressourcen gerechtfertigt werden. Die Gefahren hierbei liegen unter anderem in einer maßlosen Datenerhebung, -speicherung und -weitergabe sowie in unbefugtem Zugriff auf die Daten.[9] Ein solches Datenverarbeitungsverhalten könnte zur Verwirklichung von Foucaults Panopticon[10] führen, in dem die Bürger sowohl vom *Big Brother* (dem Staat) als auch vom *Big Browser* (dem Privaten) flächendeckend überwacht werden. Die elektronische Verarbeitung personenbezogener Daten macht es dem Einzelnen schwer oder sogar unmöglich, die Erhebung, Speicherung und Verwendung seiner Daten zu überblicken und zu kontrollieren. Die Art und Weise der Datenverarbeitung seitens des Staates kann den Lebensstil und das Kommunikationsverhalten der Bürger, folglich auch das Gemeinwohl entscheidend beeinträchtigen.[11] Gemäß dem Konzept des Panopticons unterlägen die persönlichen Entfaltungsmöglichkeiten der Bürger den Beschränkungen durch die Überwachung und Registrierung durch den Staat. Dies würde dazu führen, dass die Bürger sich der Überwachung in einem bestimmten Maße bewusst werden, sich darauf einstellen und sich den an sie gerichteten Erwartungen anpassen.[12] Werden diese bedeutenden Probleme vom Gesetzgeber nicht

9 Vgl. *Bull*, Datenschutz oder die Angst vor dem Computer, S. 242: Die Datenschützer sahen in den Ermittlungsmethoden – insbesondere z. B. in der Rasterfahndung – die Gefahr, „dass jeder in Verdacht geraten könne, auch der Fromme und Frömmste, auch der Unauffälligste."

10 Foucaults Panopticon beschreibt einen Ort, an dem jede Person vollständig beobachtet werden kann. Es beschränkt sich also nicht auf das ‚Panradicon'. Ein Panopticon ist schließlich ein Ort, an dem jede Bewegung eines anderen, unabhängig von seiner Form, sei es kreisförmig oder quadratisch, überwacht werden kann.

11 BVerfGE 65, 1 (43).

12 *Schmidt*, Die bedrohte Entscheidungsfreiheit, JZ 1974, 241, 245; Foucaults Kernprinzip beim Panopticon besteht darin, dass das Überwachungsobjekt das „Auge" der Überwachung verinnerlicht. Die Person, die in einem Panopticon überwacht wird, weiß nicht, wann der Blick der Überwachung in einem bestimmten Raum oder Bereich auf sie fallen wird. Die Überwachten verinnerlichen daher die Existenz eines solchen Blickes, sodass das Verlangen nach Aufbruch und Rebellion, das von innen heraus entstehen kann, unterdrückt wird, was dazu führt, dass

hinreichend berücksichtigt, können solche neuen Ermittlungsmethoden zu einer grenzüberschreitenden Überwachung durch den Staat führen und damit die Freiheitsrechte der Bürger gefährden. Innerhalb der Gesellschaft wächst die Besorgnis, dass sich der Verfassungsstaat als Reaktion auf die terroristische Bedrohung in einen Überwachungs- oder Präventionsstaat verwandelt.[13]

IV. Notwendiger Datenschutz

Die oben beschriebenen neuen Ermittlungsmittel generieren in der Konsequenz also auch Gefahren für den Datenschutz und die Privatsphäre. Die Standardisierung der Datenerhebung, die elektronische Datenspeicherung und deren weltweite Nutzung, der Trend zu immer detaillierteren Datensammlungen für unterschiedliche Zwecke, die zunehmende Vernetzung der Systeme und das wachsende Verlangen nach eigenmächtigem Zugriff auf die in anderen Datenbanken gespeicherten Informationen[14] gefährden den Schutz personenbezogener Daten und der Privatsphäre. Die Möglichkeiten und Gefahren der automatisierten Datenverarbeitung haben daher die Notwendigkeit des Datenschutzes deutlich hervortreten lassen. Je größer die Bedeutung der Datennutzung in einer Informationsgesellschaft wird, desto stärker bekundet die Gesellschaft ihr Interesse an Datenschutz. Es handelt sich hierbei also um ein Spannungsverhältnis zwischen der Aufgabe des Staates, für die Sicherheit seiner Bürger zu sorgen, und dem Recht auf informationelle Selbstbestimmung des Einzelnen. Der Staat ist dazu verpflichtet, die Sicherheit zu gewährleisten und zugleich die Grundrechte der Bürger zu achten. Jeder Eingriff in die Grundrechte muss in einem ausgewogenen Verhältnis zu dem gewählten Mittel und dem beabsichtigten Zweck stehen.[15] Daraus ergibt sich, dass der Staat die Sicherheit seiner Bürger durch möglichst geringe Eingriffe in die Freiheitsrechte zu gewährleisten hat. Dazu ist ein Ausgleich zwischen dem Datenschutz

---

die Regeln aus Angst vor Überwachung immer und überall eingehalten werden, selbst dann, wenn das Individuum de facto gar nicht überwacht wird.

13 *Hirsch*, Gesellschaftliche Folgen staatlicher Überwachung, DUD 2008, 87, 89; *Albrecht, P.-A.*, Vom Präventionsstaat zur Sicherheitsgesellschaft, Wege kontinuierlicher Erosion des Rechts, in: *Herzog/Hassemer* (Hrsg.), Festschrift für Winfried Hassemer; dazu kritisch *Bull*, Informationelle Selbstbestimmung – Vision oder Illusion?: Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit, S. 18.

14 *Tolzmann*, Bundeszentralregistergesetz, S. 1.

15 BVerfGE 35, 410.

einerseits und der Datennutzung zum Zweck der Verbrechensprävention oder -aufklärung andererseits erforderlich.

Als Reaktion auf eine sich zunehmend zu einer Leistungsverwaltung entwickelnden öffentlichen Verwaltung, die sich immer komplexeren Aufgabenstellungen und damit korrespondierend ständig steigenden Informationserwartungen ausgesetzt sah, erfolgte die fortschreitende Automatisierung der Datenverarbeitung. Die mit dieser Automatisierung einhergehenden Gefahren für die Persönlichkeitsrechte des Einzelnen bestehen zum einen in möglichen Fehlinformationen durch Falschverarbeitung und zum anderen im Kontextverlust durch Abtrennung abstrakter Daten von dem konkreten Lebenszusammenhang, innerhalb dessen sie erhoben worden sind, sowie in dem Informationsvorsprung, den die öffentliche Verwaltung zunehmend erhält. Diese Gefahren mussten zu sozialen und politischen Konsequenzen in Form von gesetzlichen Regelungen zum Schutz der Bürgerinnen und Bürger führen.[16] Auch das Bundesverfassungsgericht hat die der EDV immanenten Gefahren wahrgenommen und die Notwendigkeit des Schutzes davor betont.[17] Die freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung und Verwendung sowie gegen die Weitergabe seiner personenbezogenen Daten voraus. Dieser Missbrauch kann entweder innerhalb des Gesetzesrahmens erfolgen, etwa durch die Ausnutzung von Lücken in bestimmten Vorschriften, oder aber im Rahmen eines Vertrags mit Dateninhabern, die sich das Fehlen solcher Gesetze zunutze machen. Von Seiten der Gesetz-

16 *Tolzmann*, Bundeszentralregistergesetz, S. 25 ff.

17 BVerfGE 65, 1 (42 f.): „Diese Befugnis bedarf unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße des Schutzes. Sie ist vor allem deshalb gefährdet, weil bei Entscheidungsprozessen nicht mehr wie früher auf manuell zusammengetragene Karteien und Akten zurückgegriffen werden muss, vielmehr heute mit Hilfe der automatischen Datenverarbeitung Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (personenbezogene Daten [vgl. § 2 Abs. 1 BDSG]) technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar sind. Sie können darüber hinaus – vor allem beim Aufbau integrierter Informationssysteme – mit anderen Datensammlungen zu einem teilweisen oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden, ohne dass der Betroffene dessen Richtigkeit und Verwendung zureichend kontrollieren kann. Damit haben sich in einer bisher unbekannten Weise die Möglichkeiten einer Einsichtnahme und Einflussnahme erweitert, welche auf das Verhalten des Einzelnen schon durch den psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen."

gebung wurde bereits mit zahlreichen Novellierungen bestehender sowie durch die Verabschiedung neuer Gesetze auf die zunehmende elektronische Verarbeitung von Daten reagiert.

Um die Bürger vor einer übermäßigen oder unbefugten Erhebung, Speicherung, Verwendung und Weitergabe ihrer Daten zu schützen – obwohl all dies zur Effizienz von Ermittlungen beitragen mag –, sollten verfahrensrechtliche und organisatorische Sicherheitsvorkehrungen getroffen werden. Ohne diesen Schutz kann eine Person sich nicht frei entfalten. Im Zusammenhang mit diesem Ausgleich zwischen dem Datenschutz und der Datenverwendung gibt es in Deutschland bereits einige Entscheidungen des Bundesverfassungsgerichts – z. B. das Vorratsdatenspeicherungsurteil[18] oder das Volkszählungsurteil[19] – sowie einige gesetzliche Regelungen.[20,21] Einige Autoren haben sich bereits mit dem Interessenausgleich zwischen Freiheit und Sicherheit in Bezug auf das Thema Datenschutz befasst.[22] Es mangelt gleichwohl an einer rechtsvergleichenden Untersuchung oder einer Gesamttheorie sowie an grundsätzlichen Lösungsprinzipien, die in sämtlichen Stadien des Strafverfahrens Anwendung finden können. Wesentlich für jeglichen Diskurs über den Datenschutz im Strafverfahren ist die Klärung der folgenden Fragen und Faktoren: Mit welchen verfahrensrechtlichen und organisatorischen Sicherheitsvorkehrungen sind strafprozessuale Maßnahmen versehen, die personenbezogene Daten für Zwecke des Strafverfahrens nutzen? Sind die Vorkehrungen im Hinblick auf die Eingriffsintensität einer Maßnahme hinreichend, um die Freiheitsrechte der Bürger zu schützen? Darüber hinaus gibt es weitere Aspekte, die zum effektiven Schutz personenbezogener Daten unter den Bedingungen der modernen Datenverarbeitung zu beachten sind. Als Voraussetzung gilt,

18 BVerfGE 125, 260.

19 BVerfGE 65, 1: Das Volkszählungsurteil ist eine Grundsatzentscheidung des Bundes-verfassungsgerichts vom 15. Dezember 1983, mit der das Grundrecht auf informationelle Selbstbestimmung als Ausfluss des allgemeinen Persönlichkeitsrechts und der Menschenwürde etabliert wurde. Das Urteil gilt als ein Meilenstein des Datenschutzes.

20 Zum Beispiel im BDSG, TKG oder in der StPO usw.

21 In diesem Zusammenhang gibt es in den USA den Privacy Act (1974), den Electronic Communications Privacy Act (1986) und den Communications Assistance for Law Enforcement Act (1994) usw.

22 Vgl. *Bull*, Informationelle Selbstbestimmung – Vision oder Illusion?: Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit; *Wiedner-Braun*, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung – am Beispiel des personenbezogenen Datenverkehrs im www nach deutschem öffentlichen Recht; *Wiedemann*, Regieren mit Datenschutz und Überwachung.

dass es für die Betroffenen nachvollziehbar sein muss, welche ihrer Daten von wem, in welchem Verwendungszusammenhang weiterverarbeitet werden dürfen. Hierfür ist auch erforderlich, dass die Zwecke der Datenverarbeitung bereichsspezifisch und präzise festgelegt werden, d. h. die für einen bestimmten Zweck erhobenen Daten dürfen nicht ohne Weiteres für andere Zwecke an andere Stellen weitergegeben werden.

B. Forschungsziel, Forschungsmethode und Gang der Untersuchung

I. Forschungsziel

Das Forschungsziel besteht darin, einen grundsätzlichen Lösungsansatz für den Schutz und die Auswertung personenbezogener Daten im Strafverfahren zu finden. Das dient nicht nur der Analyse der vorhandenen Rechtslage des Strafrechts, sondern soll auch zur Erarbeitung verschiedener Reformvorschläge führen. Es soll dargelegt werden, ob und inwieweit persönliche Daten im Strafverfahren genutzt werden und wie sie in Zukunft im Strafverfahren geschützt werden sollten. Gegenstand der vorliegenden Untersuchung sind dabei Ermittlungsmaßnahmen im Rahmen des neuen Strafprozessrechts sowie außerhalb des Strafprozessrechts, aber es sollen auch diverse klassische Fragestellungen miteinbezogen werden.

Im Vordergrund dieser Untersuchung steht die Frage, ob und wie unter den Bedingungen der modernen Datenverarbeitung Freiheits- und Sicherheitsinteressen miteinander in Einklang gebracht werden können. Ein wesentlicher Bestandteil der Arbeit ist dabei die Untersuchung der Fragen, wie der Schutz der Privatsphäre bzw. personenbezogener Daten als ein Freiheitsgrundrecht der Bürger im Grundgesetz festgelegt ist, wie personenbezogene Daten im Strafverfahren genutzt werden, ob und inwieweit die neuen sicherheitspolitischen Instrumente, die personenbezogene Daten verwenden, mit Maßnahmen bewehrt sind, sodass die Bürger vor der unbefugten oder übermäßigen Erhebung, Speicherung und Nutzung ihrer personenbezogenen Daten geschützt werden, und ob die getroffenen Maßnahmen hinreichend sind, um die Freiheitsrechte des Einzelnen unter den Bedingungen der automatisierten Datenverarbeitung zu schützen. Denn nach dem Urteil des Bundesverfassungsgerichts vom 2. März 2010 über die Vorratsdatenspeicherung wurde die Frage, ob und wie durch das Grundgesetz ein Ausgleich zwischen Freiheit und Sicherheit erzielt

wird, der den Herausforderungen des 21. Jahrhunderts gerecht wird, neu aufgeworfen.[23]

II. Forschungsmethode

1. Gründe für die Länderauswahl

Die Untersuchungsgegenstände hinsichtlich der Forschungsfragen der vorliegenden Arbeit bilden das deutsche und das amerikanische Recht. Diese Rechtsordnungen wurden nicht nur deswegen ausgewählt, weil sie wichtige Referenzrechtsordnungen darstellen, sondern auch insbesondere im Hinblick auf ihre grundlegenden Unterschiede, die interessante rechtsvergleichende Ergebnisse versprechen. Die vorliegende rechtsvergleichende Untersuchung zielt daher insbesondere darauf ab, Hinweise auf vorbildhafte Ausgleichsregelungen zu finden. Die Auswahl soll durch die folgenden Erwägungen näher begründet werden:

Die deutsche und die US-amerikanische Rechtsordnung beruhen grundsätzlich auf unterschiedlichen rechtssystematischen Grundlagen, nämlich auf dem kontinentaleuropäischen Recht auf der einen und dem *Common Law* auf der anderen Seite. Die beiden Rechtsordnungen unterscheiden sich ferner auch in ihrer rechtspolitischen Orientierung: die sogenannte *right-dominated-policy* steht im Gegensatz zu der sogenannten *market-dominated-policy*. Es scheint interessant zu beobachten, wie die beiden Rechtsordnungen auf dieser unterschiedlichen Grundlage die Aufgabe des Datenschutzes unter den Bedingungen der modernen Datenverarbeitung wahrnehmen. Bislang wurden in der europäischen Union einige Richtlinien und Verordnungen zum Datenschutz erlassen. Aus der Feststellung seitens der EU, dass die USA im Vergleich zu den EU-Mitgliedstaaten hinsichtlich des Datenschutzes kein angemessenes Schutzniveau bieten, ergab sich die Unterzeichnung der Safe-Harbor-Vereinbarung zwischen dem US-Handelsministerium und der Europäischen Kommission. Außerdem wurde mit dem NSA-Skandal die Diskussion um das Verhältnis zwischen Freiheit und Sicherheit im digitalen Zeitalter neu entfacht. Überraschenderweise zeigte der NSA-Skandal auf, dass die USA über ein umfangreicheres Überwachungsprogramm als Deutschland verfügen oder verfügt haben. In Deutschland gibt es zwar schon rechtsvergleichende Untersu-

23 *Moser-Knierim*, Vorratsdatenspeicherung – Zwischen Überwachungsstaat und Terror-abwehr, S. 2.

chungen bezüglich anderer Mitgliedstaaten der EU,[24] jedoch fehlt es an rechtsvergleichenden Untersuchungen bezüglich der US-amerikanischen Rechtsordnung.

Die methodische Herausforderung bei diesem Ansatz besteht darin, dass aufgrund der ausgeprägten föderalistischen Struktur der USA das bundesstaatliche und das einzelstaatliche Recht nebeneinander stehen. In vielen Bereichen fehlt es daher häufig an einer umfassenden Kodifizierung auf bundesstaatlicher Ebene. Um den Vergleich des US-amerikanischen Rechts mit dem deutschen Recht sinnvoll durchzuführen, wird daher in der vorliegenden Arbeit in bestimmten Bereichen zunächst auf eine umfassende Kodifizierung auf bundesstaatlicher Ebene eingegangen. Sollten bundesstaatliche Kodifizierungen fehlen, so soll exemplarisch auf die einzelstaatlichen Regelungen zurückgegriffen werden.

2. Rechtsvergleichende Untersuchung im Rahmen des Verfassungsrechts und des einfachen Rechts

Um das Ziel der vorliegenden Arbeit zu erreichen, das darin besteht, durch eine rechtsvergleichende Untersuchung einen grundsätzlichen Lösungsansatz zu finden, ist es sinnvoll, die Rechtslagen in beiden Ländern mit den unterschiedlichen Rechtssystemen sowohl im Verfassungsrecht als auch im einfachen Recht zu untersuchen und den Datenschutz sowie die Datennutzung in beiden Rechtsordnungen miteinander zu vergleichen.

3. Untersuchung in ausgewählten Einzelbereichen: Vorratsdatenspeicherung, Rasterfahndung und Strafregister

Nach der Einführung in die Datenverwendung im Strafverfahren wird die Untersuchung in den Einzelbereichen vertieft. Zunächst wird der Themenkomplex um das Strafregister analysiert, bevor die Rasterfahndung als ein neuartiges Ermittlungsmittel in der StPO untersucht werden soll. Schließlich wird die Vorratsdatenspeicherung als ein aktueller Bereich in Bezug auf den Datenschutz und gleichzeitig als eine Maßnahme außer-

24 Zum Beispiel im Bereich der Vorratsdatenspeicherung: *Chmielewski*, Die Vorratsdatenspeicherungsrichtlinie und ihre Umsetzung in Deutschland und in Polen; *Roßnagel/Moser-Knierim/Schweda*, Interessenausgleich im Rahmen der Vorratsdatenspeicherung.

halb der StPO, also als eine Maßnahme des überstrafprozessrechtlichen Präventionsrechts beleuchtet. Obwohl die Problemstellungen hinsichtlich des Strafregisters zunächst nur in geringem Maße mit den beiden anderen Themen zusammenzuhängen scheinen, ermöglicht eine dahingehende Untersuchung einen Überblick über einen klassischen Bereich, in dem personenbezogene Daten verwendet werden, wodurch es möglich wird, ein breites Spektrum von Problemen bezüglich des Datenschutzes im Strafverfahren zu behandeln.

4. Funktionale Rechtsvergleichung bei einzelnen Maßnahmen

Methodisch soll die Untersuchung mittels einer funktionalen Rechtsvergleichung vorgenommen werden. Unvergleichbares kann nicht sinnvoll miteinander verglichen werden, und vergleichbar ist im Recht nur, was dieselbe Aufgabe, dieselbe Funktion erfüllt.[25] Daher wird ein aussagekräftiger Vergleich in Bezug auf die Verwendung und den Schutz personenbezogener Daten in den untersuchten Rechtsordnungen nur auf dem Wege eines Vergleichs derjenigen Regelungen erreicht, die in den ausgewählten Bereichen funktional dieselbe Aufgabe übernehmen. Die Gesamtlösung der untersuchten Problemstellung erfordert daher auf allen Ebenen die Erkennung sämtlicher funktionaler Äquivalente nach einer umfassenden Betrachtung der zu untersuchenden Rechtsordnungen.[26]

III. Gang der Untersuchung

Die vorliegende Arbeit lässt sich in fünf Teile gliedern:

Im ersten Teil mit dem Titel „Kollision zwischen Freiheit und Sicherheit“ werden die neuen Herausforderungen beleuchtet, die sich angesichts des Versuchs stellen, im digitalen Zeitalter sowohl Freiheit als auch Sicherheit zu gewährleisten. Hierbei wird erklärt, wie und warum sich die soziale Kontrolle in der modernen Gesellschaft verändert hat und welche neuen technikgestützten Instrumente in Strafangelegenheiten unter diesen

25 *Zweigert/Kötz*, Einführung in die Rechtsvergleichung, 3. neubearb. Aufl., 1996, S. 33.

26 *Sieber*, Strafrechtsvergleichung im Wandel: Aufgaben, Methoden und Theorieansätze der vergleichenden Strafrechtswissenschaft, in: Sieber/Albrecht (Hrsg.), Strafrecht und Kriminologie unter einem Dach, Berlin 2006, S. 112 f.

Bedingungen eingesetzt werden. Durch die Vorführung neuer technikgestützter Instrumente lässt sich nachvollziehen, in welchem Maße sich die strafrechtlichen Ermittlungsmaßnahmen im digitalen Zeitalter geändert haben. Anknüpfend an die Thematisierung der internationalen Besorgnis und der Bemühungen um den Datenschutz folgt die Untersuchung des Verhältnisses zwischen Freiheit und Sicherheit angesichts neuer Herausforderungen.

Teil zwei und Teil drei präsentieren einen Landesbericht jeweils für Deutschland und die USA bezüglich des verfassungsrechtlichen Datenschutzes und des Datenschutzes bei konkreten strafrechtlichen Maßnahmen des Strafregisters, der Rasterfahndung und der Vorratsdatenspeicherung. Es bedarf einer verfassungsrechtlichen und einfachgesetzlichen Analyse des Datenschutzes sowie der Datennutzung. Konkret wird untersucht, wie personenbezogene Daten verfassungsrechtlich geschützt werden, welche Rolle diese Daten in den ausgewählten Bereichen spielen und welche Maßnahmen bei der Nutzung dieser Daten zum Schutz des Einzelnen vor möglichen Gefahren ergriffen werden.

Im vierten Teil wird auf Grundlage der oben genannten Landesberichte der Datenschutz im Verfassungsrecht sowie hinsichtlich der konkreten Maßnahmen in beiden Ländern rechtsvergleichend untersucht. Durch diesen Rechtsvergleich sollen die Notwendigkeiten und die Mängel des Datenschutzes klar definiert werden.

Im Anschluss an die Zusammenfassung der Untersuchungen wird auf die Fragen eingegangen, wie im digitalen Zeitalter die Privatsphäre bzw. die personenbezogenen Daten als Freiheitsgrundrechte des Einzelnen verfassungsrechtlich geschützt werden sollen und welche Anforderungen auch bei Einführung neuer technikgestützter Ermittlungsmaßnahmen in einer freien Gesellschaftsordnung nicht aufgegeben werden dürfen.

Teil 1: Kollision zwischen Freiheit und Sicherheit

Die Gewährleistung von Freiheit und Sicherheit stellen zwei der wichtigsten Aufgaben des Staates dar. Neue Bedrohungslagen, damit verbundene neue gesellschaftliche Anforderungen und die stetig fortschreitende Digitalisierung sind hierbei große Herausforderungen. Durch eine Ausweitung der gesamtgesellschaftlichen Überwachung als Reaktion auf terroristische Bedrohungen ist die Gewährleistung der Sicherheit ins Zentrum der Debatte gerückt, wobei sich in Teilen der Gesellschaft die Befürchtung ausgebreitet hat, dass sich der Verfassungsstaat in einen Überwachungs- oder Präventionsstaat verwandelt.[27] Die Erfassung und Auswertung großer Mengen personenbezogener Daten soll zwar ermöglichen, zukünftigen Verbrechen vorzubeugen oder strafbare Handlungen effektiv zu verfolgen, jedoch kann das staatliche Handeln auch zu maßlosen Eingriffen in die Privatsphäre des Einzelnen führen. Das Spannungsverhältnis von Freiheit und Sicherheit hat sich durch die digitale Datenverarbeitung, Technisierung, Globalisierung und die neuen Gefährdungslagen verschärft. Dabei wird in der aktuellen Diskussion sogar vielfach die Frage gestellt, ob es nicht mittlerweile „Sicherheit statt Freiheit" heißt.[28] Erforderlich ist hierbei die Herstellung eines möglichst optimalen Ausgleichs zwischen dem Bedürfnis nach kollektiver Sicherheit und der Wahrung individueller Freiheit. In diesem Zusammenhang entfachte im 21. Jahrhundert eine kontrovers geführte Diskussion um das Verhältnis zwischen Freiheit und Sicherheit.

Die veränderten gesellschaftlichen Bedingungen stellen die frühere Sozialkontrolle in Frage: Wie können unter den Bedingungen digitaler Datenverarbeitung und unter dem Druck terroristischer Bedrohungslagen Freiheit und Sicherheit gewährleistet werden?

---

27 *Moser-Knierim*, Vorratsdatenspeicherung – Zwischen Überwachungsstaat und Terror-abwehr, S. 2; *Hirsch*, Gesellschaftliche Folgen staatlicher Überwachung, DUD 2008, 87, 89; *Albrecht, P.-A.*, Vom Präventionsstaat zur Sicherheitsgesellschaft, Wege kontinuierlicher Erosion des Rechts, in: *Herzog/Hassemer* (Hrsg.), Festschrift für Winfried Hassemer; *Huster/Rudolph*, Vom Rechtsstaat zum Präventionsstaat; *Trojanow/Zeh*, Angriff auf die Freiheit: Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte.

28 *Hornig*, Sicherheit statt Freiheit, 2010.

Zur Klärung dieser Frage soll erfasst werden, wie sich die gesellschaftlichen Bedingungen in der modernen Gesellschaft verändert haben und in welche Richtung sich die gegenwärtige Sozialkontrolle aus der strafrechtlichen Perspektive betrachtet entwickelt (I). Danach werden die neuen, aufgrund der veränderten Sozialkontrolle eingeführten technikgestützten Maßnahmen zur Sicherheitsgewährleistung vorgestellt (II). Anhand dessen lässt sich feststellen, wie ein Staat in einer modernen Gesellschaft die Sicherheit gewährleistet. Anschließend wird der Frage nachgegangen, welche Bedeutung dem Datenschutz im digitalen Zeitalter zukommt und welche Anstrengungen international hinsichtlich der Sicherstellung dieses Schutzes unternommen werden (III). Dies ist deshalb wichtig, weil die internationalen Bemühungen um die Sicherstellung des Datenschutzes als Voraussetzung für die Freiheitsgewährleistung des Einzelnen in der digitalen Zeit einen ganz entscheidenden Einfluss auf die Entwicklung und Ausgestaltung der jeweiligen nationalen Regelungen haben. Abschließend wird das gesellschaftliche Phänomen unter dem Aspekt der Kollision zwischen Freiheit und Sicherheit erklärt (IV). Dadurch soll wiederum die Notwendigkeit betont werden, diese beiden legitimen Interessen miteinander in Einklang zu bringen.

A. Neue Sozialkontrolle in der modernen Gesellschaft

Die Gegenstände und Ziele von sozialer Kontrolle sowie ihre Mechanismen und Techniken hängen von den soziokulturellen, wirtschaftlichen und politischen Strukturen und Bedingungen innerhalb einer Gesellschaft ab.[29] Was also jeweils als Bedrohung der sozialen Ordnung aufgefasst und in welcher Weise darauf reagiert werden soll, variiert mit den jeweiligen Entwicklungen der Gesellschaft.[30]

I. Sozialkontrolle im Wohlfahrtsstaat

Im 19. und 20. Jahrhundert war zumindest in Europa unter der wohlfahrtsstaatlichen Politik die Sozialkontrolle durch Disziplinierung,

29 Siehe *Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert, S. 17 m. w. N.

30 *Groenemeyer*, Wege der Sicherheitsgesellschaft, Gesellschaftliche Transformationen der Konstruktion und Regulierung innerer Unsicherheiten, S. 8.

Behandlung und Rehabilitation (Resozialisierung) von Tätern vorherrschend. Aus dieser Perspektive werden die Gründe für von sozialen Normen abweichende Verhaltensweisen in mangelnden Integrationsfähigkeiten oder -möglichkeiten der Individuen gesehen, die wiederum durch persönliche und sozialstrukturelle Defizite verursacht werden.[31] Bei diesem Modell wurde der Schwerpunkt auf die positive Spezialprävention und die negative Generalprävention gelegt. Die Resozialisierung des Täters als das alleinige Ziel des Freiheitsentzugs steht im Vordergrund, der Gesellschaftsschutz hingegen wird nur als (untergeordnete) Aufgabe des Strafvollzugs angesehen (§ 2 Strafvollzugsgesetz). Das Bundesverfassungsgericht hat das Resozialisierungsgebot sogar aus der Verfassung abgeleitet: „Von der Gemeinschaft aus betrachtet verlangt das Sozialstaatsprinzip staatliche Vor- und Fürsorge für Gruppen der Gesellschaft, die aufgrund persönlicher Schwäche oder Schuld, Unfähigkeit oder gesellschaftlicher Benachteiligung in ihrer persönlichen und sozialen Entfaltung behindert sind; dazu gehören auch die Gefangenen und Entlassenen."[32]

II. Wandel der gesellschaftlichen Strukturen

Die wohlfahrtsstaatliche Politik muss seit geraumer Zeit auf Veränderungen der gesellschaftlichen Strukturen reagieren. Infolgedessen sind neue Anforderungen an soziale Kontrolle sowie neue Möglichkeiten derselben entstanden. Die soziale Kontrolle konnte sich nur wenig auf eine wohlfahrtsstaatliche Integration mittels Disziplinierung, Behandlung und Resozialisierung verlassen.

1. Veränderte gesellschaftliche Bedingungen

Der wohlfahrtsstaatliche Integrationsansatz wurde vor allem durch eine veränderte Vorstellung von der Delinquenz zurückgedrängt: Bereits in der kriminalpolitischen Debatte der 1970er Jahre hatte sich die Anerkennung der Ubiquität von Delinquenz durchgesetzt. Damit einhergehend erhöhte sich der empirische Zweifel daran, ob die mit dem Strafrecht verfolgten Ziele – General- und Spezialprävention – tatsächlich erreicht werden kön-

31 *Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert, S. 26 f.
32 BVerfGE 35, 202 (236).

nen.[33] Daraus ergab sich ein Orientierungswandel des Strafrechts dahingehend, den Strafzweck auf die Sicherung des Täters zu richten (negative Spezialprävention) und auf eine positive Generalprävention abzustellen.

Außerdem schwinden durch die fortschreitende Globalisierung zunehmend territoriale Grenzen. Hierdurch wird nicht nur der Verkehr von Waren, Dienstleistungen, Personen, Technik und sogar kulturellen Werten internationalisiert, sondern auch die Kriminalität. Parallel dazu internationalisieren sich auch die Sicherheitspolitik und die Strukturen sozialer Kontrolle. Sicherheit kann nicht mehr durch Maßnahmen auf ausschließlich nationaler Ebene gewährleistet werden. Denn es bedarf einer internationalen Zusammenarbeit, um die grenzüberschreitende Kriminalität zu bekämpfen.

2. Neue Anforderungen

Einhergehend damit, dass eine permanente Verunsicherung die Gesellschaft beherrscht,[34] ist seit den 1990er Jahren Sicherheit international zu einem Leitmotiv kriminalpolitischer Reformen geworden. Anlass zu dieser Bewegung gaben beispielsweise der Fall Dutroux (1995)[35] und der Fall Nathalie (1996)[36]. Infolge dieser beiden Fälle wurde das Verlangen nach Sicherheit in Verbindung mit einer Diskussion um Sicherheitslücken und einer kollektiven Identifizierung mit Kriminalitätsopfern immer stärker.[37]

Die Forderung nach Sicherheit wurde durch eine Reihe von Terroranschlägen auf der ganzen Welt verstärkt. Die Angst vor erneuten Terroran-

---

33 Zusammenfassend *Albrecht, P.-A.*, Kriminologie, S. 51 ff.; *Stolle*, Das Strafrecht, seine Zwecke und seine Alternativen, in: Studentische Zeitschrift für Rechtswissenschaft, S. 27 ff.

34 *Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert, S. 38 ff.

35 *Albrecht*, *H.-J.*, Sicherheit und Prävention in strafrechtlichen Sanktionensystemen: Eine kriminologische, komparative Untersuchung. in: *Koch*, Wegsperren? – Freiheitsentziehende Maßnahmen gegen gefährliche, strafrechtlich verantwortliche (Rückfall-)Täter im internationalen Vergleich, 431 (431).

36 *Der Spiegel*, Verbrechen: Schrei der Hilflosigkeit, Der Spiegel 40/1996 v. 30.9.1996, abrufbar unter: https://www.spiegel.de/spiegel/print/d-9095363.html.

37 *Albrecht*, *H.-J.*, Sicherheit und Prävention in strafrechtlichen Sanktionensystemen: Eine kriminologische, komparative Untersuchung. in: *Koch*, Wegsperren? – Freiheitsentziehende Maßnahmen gegen gefährliche, strafrechtlich verantwortliche (Rückfall-)Täter im internationalen Vergleich, 431 (483).

schlägen rückt die Gewährleistung von Sicherheit als eine der zentralen staatlichen Aufgaben in den Vordergrund und scheint den Einzelnen dazu zu veranlassen, willentlich seine Freiheit für die Sicherheit aufzugeben. Dies zeigt sich auch ganz klar in der Befürchtung des ehemaligen Verfassungsrichters *Grimm*: „Im Kampf gegen den Terrorismus läuft der Staat Gefahr, die Freiheit der Sicherheit zu opfern."[38]

Es könnte zwar einige Gründe für die von permanenter Verunsicherung und permanentem Sicherheitsbedürfnis beherrschte Gesellschaft geben, eine wichtige Rolle spielt aber die Entwicklung der Massenmedien. Ungeachtet dessen, dass die Zahl der Kriminalitätsfälle tatsächlich nicht steigt, reagiert die Gesellschaft in Bezug auf die Gefahren von Kriminalität mit einer Verunsicherung, die angesichts der Fakten allein unerklärlich bleiben muss. Sie hat daher im Rahmen der Sicherheitsherstellung immer höhere Erwartungen an den Staat und das Strafrecht.

3. Neue technische Möglichkeiten

Neue technische Entwicklungen eröffnen viele Möglichkeiten im menschlichen Leben. Es erweist sich jedoch, dass die stetigen Fortschritte auf dem Gebiet der Wissenschaft und der Technik selbst Mittel zur Erzeugung von Großrisiken werden können. Damit wird die Sicherheit bürgerlicher Lebensbedingungen durch neue Gefahrengruppen bedroht, die durch die Entwicklung der modernen Technik hervorgerufen werden. Während die neue Technologie einerseits den Menschen mehr Wohlstand ermöglicht, kann sie andererseits aber auch zur Folge haben, dass sich die Menschen neuen Arten von Gefahren ausgesetzt sehen und solche Entwicklungen als Möglichkeiten zur Bedrohung der Sicherheit des Lebens eingesetzt werden. Angst und Furcht vor diesen neuen Gefahren- und Risikogruppen führen zu einem gesteigerten Sicherheits- und Präventionsbedürfnis, was die Schaffung neuer Strafvorschriften begünstigt.[39] Diese gesellschaftliche Veränderung drängt den Gesetzgeber dazu, Sicherheit und Prävention gegenüber Freiheit kriminalpolitisch höher zu gewichten (Tendenz des Prä-

38 *Grimm*, Aus der Balance, Die Zeit v. 28.11.2007, abrufbar unter: https://www.zeit.de/2007/49/Schaeuble-Antwort.

39 *Sieber*, Legitimation und Grenzen von Gefährdungsdelikten im Vorfeld terroristischer Gewalt – Eine Analyse der Vorfeldtatbestände im „Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten.", NStZ 2009, 353.

ventionsstrafrechts). Dabei werden die staatlichen Eingriffe zeitlich immer mehr vorverlagert, damit die Aufgaben des Staates effektiv erfüllt werden können. So entstehen beispielsweise die Kriminalisierung im Vorfeld einer Rechtsgutsverletzung sowie die Erweiterung der – abstrakten oder konkreten – Gefährdungsdelikte.[40]

Auch bei der Absicherung vor Risiken sind die technischen Fortschritte hilfreich. Die Kombination der neuen technischen Möglichkeiten mit dem steigenden Sicherheitsbedürfnis innerhalb der Gesellschaft löst im Zusammenhang mit einem neuen Mechanismus neue Methoden sozialer Kontrolle aus: eine Ausweitung und Intensivierung der Überwachung sowie die Ausforschung sozialer Lebensumstände durch staatliche und private Akteure.[41] Auf diese Weise ermöglicht die moderne automatisierte Datenverarbeitung die Verwaltung und den Umgang mit zuvor nicht handhabbaren Datenmengen. Der Risikokontrolle und der Gefahrenabwehr kommt dabei eine erhebliche Bedeutung zu. Die auf diesen Trend ausgerichtete Sicherheitsgesetzgebung wird zu einer „Querschnittsmaterie“[42], die die Freiräume der modernen Zivilgesellschaft – und damit deren Substanz – als potenzielle Gefahr versteht und somit unter Generalverdacht stellt. Dadurch bedingt nimmt auch die Einbeziehung der Zivilgesellschaft in die Kontrolle und Repression von Kriminalität zu.[43,44]

III. Sozialkontrolle der Gegenwart

Durch die oben aufgeführten Änderungen wandelt sich auch die soziale Kontrolle der Gegenwart. Die Kontrolltechnik macht nicht nur das

---

40 Gefährdungstatbestände sind zwar nicht allein der modernen Strafrechtsentwicklung geschuldet, aber im modernen Strafrecht scheint ihre Verbreitungsgeschwindigkeit mit veränderten Anwendungsbereichen sowie Legitimationsbegründungen zuzunehmen.

41 *Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert, S. 25

42 *Albrecht*, *H.-J.*, Der erweiterte Sicherheitsbegriff und seine Folgen, RAV Infobrief # 91, S. 6.

43 *Albrecht*, *H.-J.*, Der erweiterte Sicherheitsbegriff und seine Folgen, RAV Infobrief # 91, S. 16: Diese Einbeziehung verwirklicht sich besonders auf dem Gebiet der Telekommunikation.

44 *Singelnstein* befürchtet, dass man eher in eine permanente Unsicherheit gerät, wenn immer häufiger über Risikokontrolle und Gefahrenabwehr diskutiert wird (*Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert, S. 35).

Individuum, sondern auch die Gefahr und weiter das Risiko zu ihrem Gegenstand. Parallel zu den Forderungen nach Sicherheit, die in einer von Risiken und Verunsicherung beherrschten Gesellschaft in ihrer Häufigkeit und Intensität zunehmen, ändert sich auch die soziale Kontrolle. Sie setzt sich im Zusammenhang mit Gefährdungslagen zunehmend unabhängig von konkreten Anlässen oder bestimmten Personen durch.[45] Diese Gefährdungslage ist eine abstrakte Gefahr oder sogar ein Gefahrenpotenzial.

Im Anschluss an die Anwendung des Begriffs „Risikogesellschaft" von Beck werden mehrere Begriffe für diese Entwicklung sozialer Kontrolle dargelegt.[46] Nach *Legnaro*, der die gesellschaftlichen Änderungen im Jahre 1997 mit dem Begriff „Sicherheitsgesellschaft" bezeichnet hat, besitzt die Sicherheitsgesellschaft folgende Merkmale:

> „[…] dass nicht nur staatliche, sondern allmählich und in stetig zunehmendem Ausmaß auch private Akteure an der Produktion von Sicherheit teilnehmen, dass die Überwachung nicht nur dem Staatsschutz im engeren Sinne gilt, sondern Aktivitätskontrollen von allen Bürgern – tendenziell durch alle Bürger – mit dem Ziel Risikominimierung für alle angestrebt werden und dass schließlich die Produktion von Sicherheit nicht nur eine staatliche Aufgabe ist, sondern eine permanente gesellschaftliche Anstrengung, ein Regime des täglichen sozialen Lebens."[47]

Im Zusammenhang damit zeichnet sich die gegenwärtige Gesellschaft zumeist durch folgende Besonderheiten aus:[48] die Allgegenwärtigkeit der Bedrohungen von Sicherheit, die Politisierung und Entprofessionalisierung der Sicherheitspolitik, die Privatisierung und Technisierung sozialer Kontrolle, den grundlegenden Wandel der Logik politischer und staatlicher Sicherheitsproduktion weg von der Resozialisierung und Reintegration von Tätern[49] hin zu der Idee des Gesellschaftsschutzes, der Entwicklung

---

45 *Legnaro*, Konturen der Sicherheitsgesellschaft: Eine polemischfuturologische Skizze, in: Leviathan, S. 274: *die Personalisierung des Verdachts*.

46 Beispielsweise Risikogesellschaft, Sicherheitsgesellschaft, Sicherheitsstaat, Präventions-staat, Überwachungsstaat o. Ä.

47 *Legnaro*, Konturen der Sicherheitsgesellschaft: Eine polemischfuturologische Skizze, in: Leviathan, S. 271 f.

48 Vgl. *Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert.

49 Die Anwendung von Gewalt und Zwang gegen abweichendes Verhalten war für die Disziplinargesellschaft des 19. und 20. Jahrhunderts kennzeichnend. Der Begriff der Disziplinargesellschaft geht auf Foucault zurück. Die Disziplinargesellschaft war durch ein allgemein gültiges Normen- und Wertegefüge gekennzeich-

einer Kontrollkultur und der gleichzeitigen Moralisierung und Entmoralisierung abweichenden Verhaltens sowie schließlich durch ein permanentes Verunsicherungsgefühl, das allein mit dem Aspekt abweichenden oder kriminellen Verhaltens nicht erklärt werden kann.[50]

Der Wandel sozialer Kontrolle hat vor allem auf das Strafrecht einen erheblichen Einfluss. Dieser Wandel lässt sich zunächst hinsichtlich der menschlichen Erkenntnisse feststellen. Die alte kriminalpolitische Logik, dass von sozialen Normen abweichende Verhaltensweisen vor allem in bestimmten marginalen Klassen vorkommen und dass darauf mit der Politik der Resozialisierung reagiert werden sollte, wurde durch die neue Erkenntnis abgelöst, dass Verbrechen nicht nur durch Personen aus diesen Kreisen, sondern durch solche aus allen Schichten der Gesellschaft begangen werden (Ubiquität von Delinquenz).[51]

Ein empirischer Erfolgsnachweis über die Erreichung der angestrebten Ziele ist jedoch nicht möglich. Es fehlen vor allem sichere empirische Belege dafür, dass das Strafrecht negative Generalprävention und positive Spezialprävention erreichen kann.[52] Vielmehr zeigt beispielsweise eine Untersuchung von Martinson und seiner Feststellung *nothing works*,[53] dass die Resozialisierungsstrategie zu keinem Erfolg führt. Ferner ergaben empirische Untersuchungen, dass die Rückfallquoten umso höher ausfallen, je schwerer und höher die verhängte Strafe ist[54] und dass eine formelle Sanktionierung bei Jugendlichen sich eher kontraproduktiv auswirkt.[55]

Diese Erkenntnisse stellen das Strafrecht in seiner bisherigen Form in Frage. Die Form der Informationsbeschaffung zur Strafverfolgung und zur polizeirechtlichen Gefahrenabwehr wurde angesichts neuer technischer

---

net, bei dessen Verletzung das Individuum diszipliniert und an der präskriptiven Norm ausgerichtet wurde (vgl. *Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert, S. 62 und 119).

50 *Groenemeyer*, Wege der Sicherheitsgesellschaft, Gesellschaftliche Transformationen der Konstruktion und Regulierung innerer Unsicherheiten, S. 15 ff.

51 *Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert, S. 20.

52 *Albrecht*, *H.-J.*, Sicherheit und Prävention in strafrechtlichen Sanktionensystemen: Eine kriminologische, komparative Untersuchung. in: *Koch*, Wegsperren? – Freiheitsentziehende Maßnahmen gegen gefährliche, strafrechtlich verantwortliche (Rückfall-)Täter im internationalen Vergleich, 431, S. 448 m. w. N.

53 *Martinson*, What Works? – Questions and Answers About Prison Reform. The Public Interest Issue 35, 1974, 22–54.

54 *Jehle/Heinz/Sutterer*, Legalbewährung nach strafrechtlichen Sanktionen. Eine kommen-tierte Rückfallstatistik, 51 ff.

55 *Albrecht*, *P.-A.*, Jugendstrafrecht, 50 ff.

Möglichkeiten und sicherheitspolitischer Bedürfnisse beständig ausgebaut. Die soziale Kontrolle, die sich lange Zeit überwiegend auf die Täter und ihre Veränderung durch Abschreckung, soziale Dienste und Sozialpolitik bezog, wird in vielen Bereichen durch Orientierung an der Kontrolle von Situationen ersetzt, die, wenn möglich, mit Hilfe automatisierter Techniken durchgeführt werden soll. Hier steht vor allem die möglichst frühzeitige Identifizierung von Risiken im Vordergrund. Um die Sicherheit der Gesellschaft zu gewährleisten, zeichnet sich im Rahmen des materiellen Rechts vor allem die Tendenz zu einer Vorverlagerung des strafrechtlichen Schutzes durch abstrakte Gefährdungsdelikte und durch überindividuelle Rechtsgüter ab. In der gegenwärtigen Gesellschaft werden daher häufig präventive Maßnahmen ergriffen. Bezüglich solcher präventiven Maßnahmen stellt *Singelnstein* fest, der Hauptzweck solcher Techniken bestehe „in dem räumlichen Fernhalten der ‚Gefährlichen' und in der sozialen Ausgrenzung der ‚Überflüssigen'."[56] Zu diesen Zwecken nutzt das Strafrecht darüber hinaus auch die neuen technischen Möglichkeiten, die zur Optimierung der Strafverfolgung eingesetzt werden.

Unter dieser veränderten Sozialkontrolle werden im Rahmen der Strafverfolgung neue technikgestützte Maßnahmen eingesetzt, um eine Optimierung der Ermittlung zu erreichen und strafverfahrensrechtliche Maßnahmen effektiv durchzusetzen. Dies hat der technische Fortschritt ermöglicht. Mit Hilfe der modernen automatisierten Datenverarbeitung versucht das Strafrecht, schon im Vorfeld mit Risiken umzugehen, beispielsweise, indem ohne Anfangsverdacht flächendeckend ermittelt wird oder indem Maßregeln nicht durch Verurteilung, sondern durch die Feststellung eines Risikos ergriffen werden. Hierbei spielen personenbezogene Daten eine maßgebliche Rolle. Die veränderte strafrechtliche Orientierung, die neuen Forderungen der Gesellschaft nach Sicherheit und die neue Technik, die in der Lage ist, mit beträchtlichen Datenmengen umzugehen, führen jedoch auch zu neuen Herausforderungen – vor allem zur Aufgabe von Freiheit.

B. Neue technikgestützte Maßnahmen zur Sozialkontrolle

Die Feststellung und die Durchsetzung eines im Einzelfall bestehenden staatlichen Strafanspruchs zur Sicherung der gesellschaftlichen Ordnung

56 *Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert, S. 87.

setzen die Wahrheitsfindung und die Erforschung des Sachverhalts voraus, welcher der Straftat zugrunde liegt. Dies kann oftmals auch durch die Ermittlung im privaten Umfeld der verdächtigen Person und durch die Suche nach entsprechenden personenbezogenen Informationen geschehen. Dafür stehen den Strafverfolgungsbehörden zahlreiche spezielle Ermittlungsbefugnisse zur Verfügung, mittels derer auch in die Privatsphäre der Menschen eingegriffen werden kann. Denn deren Privatsphäre wird zwar grundrechtlich garantiert, unter bestimmten Einschränkungen darf jedoch in sie eingegriffen werden. Mit diesen Befugnissen kann auf den privaten Lebensbereich eines Menschen, insbesondere auf seine personenbezogenen Daten, zugegriffen werden. Im Zusammenhang mit der Sicherheitspolitik und der fortgeschrittenen Technik sind diese Befugnisse zu einer erheblichen Kraft geworden. Der technische Fortschritt ermöglicht es nun, zuvor nicht handhabbare Datenmengen miteinander zu vergleichen und zu analysieren sowie auch den privaten Raum oder das nichtöffentlich gesprochene Wort zur Kenntnis zu nehmen, wenn die Strafverfolgungsbehörden darauf bestehen.

Um zu klären, in welcher Weise die fortgeschrittene Technik in der Praxis genutzt und damit die Optimierung der Strafverfolgung erhöht wird – d. h. inwieweit die Gesellschaft heutzutage die Eingriffe dieser Maßnahmen in die Privatsphäre eines Menschen duldet –, sollen anschließend die neuen technikgestützten Maßnahmen übersichtlich vorgestellt werden.

I. Der Lauschangriff

Um insbesondere im Hinblick auf die Organisierte Kriminalität ein Eindringen in die Kernbereiche von Organisationen und somit eine Offenlegung der Strukturen zu ermöglichen, wird in der Praxis der sogenannte Große Lauschangriff eingesetzt. Darunter wird das heimliche Abhören und Aufzeichnen von den innerhalb der Wohnungen der überwachten Individuen stattfindenden Lebensvorgängen, insbesondere des dort nichtöffentlich gesprochenen Wortes, unter Zuhilfenahme technischer Mittel verstanden.[57] Dies kann sowohl in der Wohnung selbst geschehen, etwa durch einen dort versteckten Miniatursender („Wanze"), als auch

57 *Bludovsky*, Rechtliche Probleme bei der Beweiserhebung und Beweisverwertung im Zusammenhang mit dem Lauschangriff nach § 100 c Abs. 1 Nr. 3 StPO, S. 21 f.; *Geis*, Großer Aufwand für großen Lauschangriff, JuS 1998, 1174, 1174; *Müller*, Der sogenannte „Große Lauschangriff", Eine Untersuchung zu den

von außerhalb, beispielsweise mit Hilfe von Richtmikrofonen.[58] Zu den herkömmlichen Ermittlungsmethoden, die ähnlichen Zwecken wie dem Lauschangriff dienen, zählt die Telefonüberwachung oder der Einsatz von verdeckt ermittelnden Personen. Der Einsatz des Großen Lauschangriffs beruht auf der Erwägung, dass die herkömmlichen Ermittlungsmethoden, verglichen mit dem heutigen Stand der Organisierten Kriminalität, als nicht hinreichend angesehen werden.

Abzugrenzen vom Großen Lauschangriff ist der Kleine Lauschangriff, sprich, die Überwachung des nichtöffentlich gesprochenen Wortes mit technischen Mitteln außerhalb von Wohnungen. Diese Ermittlungsmethode wird oft zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität eingesetzt. Denn die herkömmlichen Ermittlungs- und Aufklärungsmethoden wurden mit Blick auf die besonderen Strukturen der Organisierten Kriminalität und die fortschreitende Professionalisierung der Straftäter in diesem Bereich als nicht mehr ausreichend angesehen.[59] Zur Durchführung dieser Überwachung werden z. B. versteckte Mikrofone und Aufzeichnungsgeräte als technische Mittel genutzt.[60]

Mit diesen beiden Arten von Lauschangriffen wurden unter bestimmten Voraussetzungen Gespräche von Personen sowohl innerhalb als auch außerhalb der Wohnung zum Gegenstand der heimlichen Ermittlung gemacht. Als Folge kann in der heutigen Welt nicht mehr darauf vertraut werden, dass ein nichtöffentlich gesprochenes Wort niemals an die Öffentlichkeit gelangt.

Rechtsproblemen der Einführung der elektronischen Wohnraumüberwachung zur Beweismittelgewinnung, S. 5.

58 *Bludovsky*, Rechtliche Probleme bei der Beweiserhebung und Beweisverwertung im Zusammenhang mit dem Lauschangriff nach § 100 c Abs. 1 Nr. 3 StPO, S. 23; *Glauben*, Kann der „Große Lauschangriff" zulässig sein? Ein Überblick über die verfassungsrechtlichen Aspekte, DRiZ 1993, 41.

59 *Paa*, Der Zugriff der Strafverfolgungsbehörden auf das Private im Kampf gegen schwere Kriminalität, S. 187.

60 *Gercke*, HK-StPO, § 100f Rn. 4; *Schmitt*, Strafprozessordnung, § 100f Rn. 4.

II. Die Überwachung der Telekommunikation

Die Strafverfolgungsbehörden können die Telekommunikation[61] zu Zwecken der Sachverhaltserforschung oder der Ermittlung des Aufenthaltsortes des Beschuldigten überwachen und aufzeichnen. Mit dieser Befugnis können nicht nur die herkömmlichen Formen des Telefonierens und Fernschreibens, sondern auch die Datenübermittlung mittels neuerer Techniken wie Mobilfunk, Satellitenübertragung, Bildtelefon oder Text- und Bildübermittlungsdiensten sowie der Kommunikation in Computernetzen wie etwa per E-Mail-Verkehr oder Online-Kommunikation überwacht werden.[62] Die Telekommunikationsüberwachung wird in fast allen Staaten von den Regierungen erlaubt, auch wenn sie hinsichtlich solcher Faktoren wie z. B. den Bedingungen, unter denen dies geschehen darf, und ob nur die Verbindungsdaten oder auch die Inhalte überwacht werden dürfen, unterschiedlich geregelt ist.

Davon abzugrenzen ist die Vorratsdatenspeicherung, nämlich die Verpflichtung der Anbieter von Telekommunikationsdiensten zur Speicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, ohne dass ein einzelfallbezogener Anlass dazu besteht. Die im Zuge der Vorratsdatenspeicherung erfassten Daten können zu einem späteren Zeitpunkt zur Telekommunikationsüberwachung genutzt werden. Die Verpflichtung zur Speicherung von Verkehrsdaten soll verhindern, dass strafrechtliche Ermittlungen nicht weiterverfolgt werden können, weil die Telekommunikationsdienstanbieter die Verkehrsdaten entweder direkt nach Rechnungsstellung gelöscht oder sie mangels Berechtigung gar nicht erst erhoben haben.[63]

Der Zugriff der Strafverfolgungsbehörden darf sich damit auch auf die Datenübermittlung mittels Techniken erstrecken. Die Behörden dürfen z. B. Kenntnis darüber erlangen, wer, wann, mit wem, auf welche Weise und wie oft kommuniziert hat. Das Gefährdungspotenzial dieser Eingriffe

---

61 Nach § 3 Nr. 22 TKG i. V. m. § 3 Nr. 23 TKG ist „Telekommunikation der technische Vorgang des Aussendens, Übermittelns und Empfangens von Signalen mittels Telekommunikationsanlagen, d. h. mittels technischer Einrichtungen oder Systeme, die als Nachrichten identifizierbare elektromagnetische oder optische Signale senden, übertragen, vermitteln, empfangen, steuern oder kontrollieren können."

62 *Schmitt*, Strafprozessordnung, § 100a Rn. 6 ff.; *Bruns*, KK-StPO, § 100a Rn. 16 ff.; *Hauck*, LR-StPO, § 100a Rn. 59.

63 BT-Drs. 16/5846, S. 31.

ist deshalb sehr hoch, weil die Aussagekraft der hier erhobenen Daten erheblich ist, da aus ihnen oder aus deren Kombination mit anderen Daten umfassende Bewegungs- und Persönlichkeitsprofile erstellt werden können.

III. Der IMSI-Catcher

Mit einem speziellen Messtechnikgerät, dem sogenannten IMSI-Catcher, lassen sich die digitale Kennung eines Mobilfunkgeräts, genauer gesagt die IMSI[64] und die IMEI[65], sowie dessen genauer Standort ermitteln.[66] IMSI-Catcher machen sich die Tatsache zunutze, dass Mobilfunktelefone in eingeschaltetem Zustand in regelmäßigen Abständen die IMSI und die IMEI an die nächste Basisstation der Funkzelle senden, in der sie sich aktuell befinden. Ein bekanntes Beispiel für einen solchen IMSI-Catcher ist der vom FBI genutzte „Stingray". Der Einsatz eines IMSI-Catchers kommt vor allem dann in Betracht, wenn bekannt ist, dass an einem bestimmten Ort Mobilfunktelekommunikation betrieben wird, jedoch keine näheren Erkenntnisse über die Identität der verdächtigen Person, das verwendete Mobiltelefon oder die Rufnummer vorliegen – etwa weil sich der zu Überwachende ein Mobiltelefon von einem Unbekannten geliehen, die Chipkarte ausgetauscht oder eine Karte unter falschen Personaldaten gekauft hat.[67]

IMSI-Catcher ermöglichen die Ermittlung der Geräte- und Kartennummer sowie des Standorts eines Mobiltelefons, aber auch das Mithören laufender Mobilfunkgespräche in Echtzeit, wenn auch mit Hilfe einer speziellen Software.

---

64 Die *International Mobile Subscriber Identity* (Kartennummer) ist eine weltweit gültige Kennung, die den Teilnehmer als Vertragspartner eines Netzbetreibers eindeutig identifiziert. Sie ist auf der Chipkarte gespeichert, die ein Mobilfunkteilnehmer bei Abschluss eines Vertrages erhält (hierzu *Bär*, Handbuch zur EDV-Beweissicherung im Strafverfahren, S. 188).

65 Die *International Mobile Station Equipment Identity* ist die weltweit nur einmal vergebene Geräte- oder Seriennummer eines Mobiltelefons. Sie ist fest mit dem jeweiligen Endgerät verbunden, sodass dieses anhand der IMSE eindeutig identifiziert werden kann (hierzu *Bär*, TK-Überwachung, S. 372).

66 *Schmitt*, Strafprozessordnung, § 100i Rn. 1.

67 *Fos*, Der IMSI-Catcher, DuD 2002, 212, 213; *Hilger*, Gesetzgebungsbericht – §§ 100g, 100h StPO, die Nachfolgeregelungen zu § 12 FAG, GA 2002, 228, 557; *Schmitt*, Strafprozessordnung, § 100i Rn. 1; *Ronellenfitsch*, Datennotwehr, DuD 2008, 110, 114.

IV. Die Rasterfahndung

Für Zwecke der Strafverfolgung werden bereits vorhandene, personenbezogene Datenbestände, die von öffentlichen und nichtöffentlichen Stellen ohne den Bezug zu Strafverfolgungsbehörden für von der Strafverfolgung unabhängige Zwecke erhoben wurden, computergestützt nach bestimmten tätertypischen Prüfungsmerkmalen (Rastern) überprüft und abgeglichen. Durch diesen Abgleich sollen Nichtverdächtige ausgeschlossen sowie Personen identifiziert werden, die weitere für die Ermittlungen bedeutsame Prüfungskriterien erfüllen. Mit Hilfe der Ermittlungsmethode der Rasterfahndung, bei der die Möglichkeit der automatisierten Datenverarbeitung für Zwecke der Strafverfolgung genutzt wird, sollen Hinweise und Spuren gefunden werden, die nach kriminalistischer Erfahrung zur Aufklärung einer Straftat beitragen können. Diesen Hinweisen und Spuren wird anschließend auf herkömmliche Weise weiter nachgegangen.[68]

Anders als beim üblichen polizeilichen Datenabgleich, bei dem der Polizei bereits zur Verfügung stehende Daten miteinander abgeglichen werden, werden bei der Rasterfahndung polizei-externe Daten, die aus anderen Gründen an anderen Stellen gespeichert sind, maschinell abgeglichen, um eine Straftat aufzuklären. Dies beruht darauf, dass der technische Fortschritt es ermöglicht, zuvor nicht handhabbare Datenmengen maschinell zu verarbeiten. Bei diesem Vorgehen werden zunächst alle auf diese Weise erfassten Personen, auf die bestimmte Merkmale zutreffen, verdächtigt.

V. Die DNA-Analyse

Die Speicherung von DNA-Identifizierungsmustern zwecks künftiger Strafverfolgung ist inzwischen eine weltweit verbreitete und häufig angewendete Ermittlungsmethode. Unter bestimmten Bedingungen dürfen die Strafverfolgungsbehörden dem Beschuldigten zur Identitätsfeststellung in einem anderen, zukünftigen Strafverfahren Körperzellen entnehmen und molekulargenetisch untersuchen. Die so erhobenen Daten dürfen in einer sogenannten DNA-Datenbank gespeichert werden. Zweck dieser Maßnahme ist es, durch eine schnellere Täteridentifizierung eine bessere Aufklärung von schweren Straftaten, insbesondere Sexualstraftaten, zu erreichen.[69]

---

68 BT-Drs. 12/989, S. 36.
69 Beispielsweise siehe BT-Drs. 13/10791, S. 4.

Ein großes Problem bei der DNA-Analyse liegt darin, dass bei ihr auf äußerst sensible personenbezogene Informationen zugegriffen wird, die eigentlich dem unantastbaren Bereich der menschlichen Persönlichkeit zuzuordnen sind, da die DNA Trägerin genetischer Informationen ist und damit sozusagen den Schlüssel zum Kern der Persönlichkeit eines Menschen darstellt. Dennoch wird weltweit zu Zwecken der Strafverfolgung häufig auf die DNA-Analyse zurückgegriffen, auch wenn ihre Verwendung von bestimmten Voraussetzungen abhängt.

VI. Die Online-Durchsuchung

Unter dem Begriff „Online-Durchsuchung" versteht man den verdeckten Zugriff staatlicher Behörden auf fremde informationstechnische Systeme über Kommunikationsnetze. Als Objekte dieser Art der Durchsuchung kommen alle von einem Mikroprozessor gesteuerten Geräte in Betracht, z. B. PCs und Mobiltelefone, aber auch elektronische Terminkalender. Die Online-Durchsuchung umfasst sowohl den einmaligen Zugriff auf den Datenbestand eines Systems als auch die sich über einen längeren Zeitraum erstreckende Online-Überwachung. Letztere ermöglicht es den Behörden, sich ein umfassendes Bild von der Nutzung des überwachten Systems zu machen. Die Online-Überwachung unterscheidet sich insofern von der Telekommunikationsüberwachung, als nicht allein der Datentransfer ausfindig gemacht wird, sondern die laufende Kommunikation der Zielpersonen direkt am Endgerät mittels Spionagesoftware überwacht wird, beispielsweise anhand eines sogenannten *Trojaner*-Programms. Trotz der heftigen Kritik an dieser Methode, die auf Eingriffe in die Grundrechte, die technischen Bedenken sowie das Missbrauchspotenzial abhebt, wird die Online-Durchsuchung in einigen Staaten[70] genutzt.

Im digitalen Zeitalter, in dem infolge der stetig steigenden Zahl von PC viele Daten mit Hilfe von Informationssystemen verarbeitet werden, könnte die Online-Durchsuchung zu ähnlichen Ergebnissen führen wie die Überwachung des Denkinhalts eines Menschen. Die Angst davor, dass die Gedanken eines Einzelnen überwacht werden könnten, kann einen enormen Einfluss auf seine Handlung nehmen. Darin liegt der bedenklichste Punkt der Online-Durchsuchung.

70 Zum Beispiel Deutschland, Österreich, Frankreich, die USA, China usw.

C. Der Schutz personenbezogener Daten

Der Einsatz technikgestützter Ermittlungsmittel zielt auf die effektive Gewährleistung der Sicherheit ab. Trotz des Erfolgs beim Einsatz solcher technikgestützter Ermittlungsmittel bei der effektiven Sicherheitsgewährleistung muss die Frage gestellt werden, ob beim Einsatz dieser Mittel ein angemessener Schutz personenbezogener Daten sichergestellt werden kann. Der Datenschutz steht im Hinblick auf die Freiheit des Einzelnen im Vordergrund. Er spielt insbesondere in der heutigen Zeit als eine Voraussetzung für die Freiheit eine wichtige Rolle.

Es ist hierbei erforderlich zu untersuchen, welche Bedeutung den personenbezogenen Daten im modernen Rechtsstaat zukommt. Anschließend soll analysiert werden, welche Bestrebungen von internationalen Organisationen unternommen werden, um personenbezogene Daten zu schützen. Die Untersuchung kann dazu dienen, die Bedeutung personenbezogener Daten zu verdeutlichen und zu betonen.

I. Die Bedeutung der Daten unter den Bedingungen der modernen automatisierten Datenverarbeitung

Die moderne automatisierte Datenverarbeitung eröffnet einerseits viele Möglichkeiten bei Ermittlungen und hilft dabei, Straftaten effektiv zu verfolgen. Sie schafft andererseits aber auch neue Herausforderungen beim Umgang mit personenbezogenen Daten. In der Informationsgesellschaft erlangen nicht nur der Austausch und die Auswertung, sondern auch der Schutz personenbezogener Daten immer mehr Bedeutung. Unter dem Begriff der *personenbezogenen Daten* sind gemäß § 3 Abs. 1 BDSG „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)“ zu verstehen. Der Begriff der persönlichen oder sachlichen Verhältnisse umfasst die körperlichen und geistigen Eigenschaften und Verhaltensweisen, die beruflichen, wirtschaftlichen, sozialen oder privaten Beziehungen sowie alle identifizierbaren Angaben wie etwa die Adresse, die Angaben als Kfz-Halter, das Bankguthaben, die Berufsbezeichnung, Krankheiten, Kreditdaten, Straftaten usw. Die Sensibilität oder Aussagekraft dieser Angaben ist für ihre Einordnung als personenbezogene Daten nicht relevant.[71] Gemäß der deutschen Rechtsprechung gibt es wegen der der Informationstechnologie

71 *Plath*, DSGVO/BDSG Kommentar, § 3 Rn. 8 m. w. N.

inhärenten Verarbeitungs- und Verknüpfungsmöglichkeiten unter den Bedingungen der automatischen Datenverarbeitung *sogar kein belangloses Datum* mehr.[72] Es besteht die Möglichkeit, aus den Daten umfassende Bewegungs- und Persönlichkeitsprofile zu erstellen. Auch wenn die jeweiligen Daten für sich allein genommen im Grunde unbedeutend und harmlos erscheinen mögen, besteht die Gefahr, dass aus deren Kombination mit anderen Daten ein Persönlichkeitsprofil eines Einzelnen hergestellt wird, was auf erhebliche Eingriffe in dessen Persönlichkeitsrecht hinauslaufen kann. Dies führt dazu, dass der Einzelne zunehmend *gläsern* wird.[73] Anders als bei anderen Grundrechten scheint sich eine Vielzahl von Menschen trotz des hohen Gefährdungspotenzials dieses Eingriffs der potenziellen Verletzung ihres Persönlichkeitsrechts im Alltag nicht bewusst zu sein. Eingriffe können infolgedessen immer häufiger und immer intensiver erfolgen.

Das Recht auf Schutz der Privatsphäre i. w. S.[74] ist ein national wie international anerkanntes Grundrecht und wird in fast allen Staaten der Welt geschützt, sei es verfassungsrechtlich oder einfachgesetzlich oder aber durch Gerichte gemäß allgemeiner Prinzipien und Werte.[75] Die personenbezogenen Daten spielen beim Schutz der Privatsphäre eine bedeutende Rolle. Auch der Datenschutz[76] gewinnt derzeit immer mehr an Bedeutung. Damit stellt sich die Frage, *wie und inwiefern personenbezogene Daten geschützt werden sollten*. Aus dieser Erkenntnis ergeben sich die nationalen sowie die internationalen Bemühungen um einen effektiven Datenschutz.

II. Internationaler Datenschutz

Jeder Staat bemüht sich darum, die individuelle Freiheit seiner Bürger zu schützen. Im digitalen Zeitalter wird versucht, personenbezogene Da-

72 BVerfGE 65, 1 (28).

73 *Comans*, Ein „modernes" europäisches Datenschutzrecht – Bestandsaufnahme und Analyse praktischer Probleme des europäischen Datenschutzes unter besonderer Berücksichtigung der Richtlinie zur Vorratsdatenspeicherung, S. 66.

74 Siehe auch http://www.privacyinternational.org/survey/rankings2007/phrcomposort.pdf, http://www.privacyinternational.org/article.shtmal?cmd[347]=x-347-563326.

75 *Genz*, Datenschutz in Europa und den USA, S. 7.

76 Der Begriff „Datenschutz" ist dabei missverständlich. Denn das Datenschutzrecht verfolgt nicht den Zweck, die auf einem „Träger" gespeicherten Daten, sondern den Einzelnen vor Verletzungen seiner Privatsphäre durch einen unzulässigen Umgang mit ihn betreffenden Daten zu schützen (vgl. § 1 Abs. 1 Nr. 1 BDSG; Art. 1 Abs. 1 Richtlinie 95/46/EG.).

ten als eine Voraussetzung für die individuelle Freiheit zu schützen. Die Staaten ergreifen dabei zwar auf nationaler Ebene Maßnahmen zum Datenschutz, stoßen dabei allerdings häufig an teilweise unüberwindbare Grenzen. Ist der Schutz personenbezogener Daten auf nationales Recht beschränkt, kann nur ein ungenügender oder sogar mangelnder Erfolg erzielt werden, da die Grenzüberschreitung des Datenverkehrs durch die zunehmende Globalisierung, die fortschreitende Technisierung, das Internet, die stetig steigende Anzahl und Nutzung von Personal Computern, die wachsende wirtschaftliche Bedeutung des internationalen Datentransfers sowie durch die sich neu ergebenden Vermarktungsmöglichkeiten immer einfacher erfolgt. Trotz dieses Umstands besteht noch immer kein allgemeiner und international gültiger Rechtsrahmen für den Datenschutz. Die Staaten trafen jedoch internationale Vereinbarungen, um die jeweiligen diversen nationalen Regelungen für den Datenschutz miteinander zu verbinden und bestehende Lücken zu schließen.[77] Diese internationalen Vereinbarungen beeinflussen wiederum die Entwicklung und die Ausgestaltung nationaler Regelungen. So wurden diese internationalen Vereinbarungen zur Grundlage der Datenschutzgesetze der einzelnen Länder.

1. Die Vereinten Nationen

Bereits die am 10. Oktober 1948 von der UN-Generalversammlung beschlossene Allgemeine Erklärung der Menschenrechte (AEMR)[78] misst der Privatsphäre der Menschen eine große Bedeutung zu. Im Art. 12 der Menschenrechtserklärung heißt es: „Niemand darf willkürlichen Eingriffen in sein Privatleben, seine Familie, sein Heim oder seinen Briefwechsel noch Angriffen auf seine Ehre und seinen Beruf ausgesetzt werden."

Basierend auf dem nationalen Verständnis des Privatsphärenschutzes beinhaltet dies die notwendigen Bedingungen für die Anknüpfung an einen spezifischen internationalen Datenschutz. Die Vereinten Nationen begriffen, dass die Privatsphäre der Menschen durch die automatisierte Verarbeitung personenbezogener Daten gefährdet werden kann und daher

77 Beispielhaft dafür sind die „Safe Harbor Principles", die im Rahmen des Art. 25 der EU-Datenschutzrichtlinie am 21. Juli 2000 zwischen den USA und der Europäischen Union vereinbart wurden.

78 Resolution 217 (III) Universal Declaration of Human Rights in: United Nations, General Assembly, Official Records Third Session (part I) Resolutions (Doc. A/810).

deren Schutz notwendig ist. Aufgrund dieser Überlegung verabschiedete die UN-Generalversammlung am 14. Dezember 1990 die „Guidelines for the Regulation of Computerized Personnel Data Files" (A/RES/45/95), zu Deutsch die „Richtlinie zur Verarbeitung personenbezogener Daten in automatisierten Dateien". Sie fordert die Mitgliedstaaten zwar dazu auf, verbindliche nationale Rechtsvorschriften für die automatisierte Verarbeitung personenbezogener Daten zu schaffen, hat als Empfehlung jedoch keine bindende völkerrechtliche Wirkung. Dennoch sind die Ergebnisse der UN-Generalversammlungen beachtenswert, da Grundsätze wie *Rechtmäßigkeit der Datenverarbeitung, Richtigkeit der Daten, Zweckbestimmung und Einsichtnahme durch die Betroffenen* auf nationale datenschutzgesetzliche Regelungen eingewirkt haben.

2. OECD

Aufgrund des zunehmenden grenzüberschreitenden Datenverkehrs und der wachsenden wirtschaftlichen Bedeutung des internationalen Datentransfers verabschiedete die Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) im Jahr 1980 die Richtlinien über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten,[79] um einen international einheitlichen Standard zu schaffen. Die Ziele dieser Richtlinien sind die Harmonisierung der Datenschutzbestimmungen der Mitgliedstaaten, die Förderung des freien Datenaustauschs sowie die Vermeidung ungerechtfertigter Handelshemmnisse.[80]

---

79 OECD, Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data (1980), Document C (80) 58 (Final), Bekanntgabe Banz, Amtl. Teil v. 14.11.1981, Nr. 215; siehe auch OECD, Recommendation on Cross-border Co-Operation in the Enforcement of Laws Protecting Privacy (2007).

80 Der Zweck der OECD-Richtlinie ist in der Präambel klar angegeben: „Im Zuge der Einführung der Informationstechnologien in verschiedene Bereiche der Wirtschaft und Gesellschaft und mit der zunehmenden Bedeutung und Leistungsstärke der elektronischen Datenverarbeitung beschloss die Organisation für Wirtschaftliche Zusammenarbeit und Entwicklung (OECD) 1980, Richtlinien für eine internationale Politik über Datenschutz und grenzüberschreitende Ströme personenbezogener Daten herauszugeben. Die rasch alle Bereiche durchdringende Entwicklung der Informations- und Kommunikationstechnologien, gekennzeichnet durch Erscheinungen wie das Internet, trug in jüngster Zeit zur beschleunigten Entstehung einer globalen Informationsgesellschaft bei. Die OECD hat sich daraufhin mit der Frage befasst, wie diese Richtlinien im 21.

Diesen Leitlinien kommt insofern eine besondere Bedeutung zu, als ihre Intention nicht nur in dem Bestreben besteht, die Privatsphäre des Individuums zu schützen. Stattdessen konzentrieren sich die Leitlinien erstmals auf den wirtschaftlichen Aspekt der Daten. Bei den Leitlinien handelt es sich aber nicht um bindendes Völkerrecht. Die Mitgliedstaaten sind nicht zur Umsetzung der Vorgaben in ein nationales Datenschutzrecht verpflichtet.

3. Europarat

Der Europarat wurde am 5. Mai 1949 von den Mitgliedern der Westeuropäischen Union (WEU) gegründet. Die Zielsetzung besteht vor allem darin, auf der Grundlage der Europäischen Menschenrechtskonvention (EMRK) einen effizienten Menschenrechtsschutz zu realisieren.[81] Bei der Entwicklung eines ungeschriebenen Grundrechtsstandards als eines Teils der allgemeinen Rechtsgrundsätze des Gemeinschaftsrechts wurde vom EuGH immer wieder auf die EMRK zurückgegriffen.[82] Sie gilt gemäß Art. 6 Abs. 3 EU zusammen mit dem Lissabon-Vertrag als ein allgemeiner Grundsatz des EU-Rechts.[83]

Nach Art. 8 Abs. 1 EMRK wird der Anspruch einer jeden Person auf Achtung ihres Privat- und Familienlebens sowie ihrer Wohnung und ihrer Korrespondenz gewährleistet. Auf der Grundlage dieser Vorschrift hat der Europarat im Jahre 1979 das international verbindliche Übereinkommen zum Schutz des Menschen bei der automatischen Verarbeitung personenbezogener Daten, das kurz „Konvention 108" genannt wird, verabschiedet. Der Konvention 108 kommt insofern eine große Bedeutung zu, als sie die erste internationale Datenschutzregelung darstellt, die für die ver-

---

Jahrhundert bestmöglich umgesetzt werden können, um die Achtung der Privatsphäre und den Schutz personenbezogener Daten online zu gewährleisten."

81 Die Konvention zum Schutz der Menschenrechte und der Grundfreiheiten wurde am 4. November 1950 in Rom abgeschlossen und ist nach Ratifizierung von zehn Staaten am 3. September 1953 in Kraft getreten (vgl. BGBl. 1952 II, S. 686).

82 EuGH, Rs. 44/79, Slg. 1979, 3727 Rn. 17 ff.

83 Art. 6 Abs. 3 EU verweist ausdrücklich auf die EMRK: „Die Union achtet die Grundrechte, wie sie in der [...] Europäischen Konvention zum Schutze der Menschenrechte und Grundfreiheiten gewährleistet sind und wie sie sich aus den gemeinsamen Verfassungsüberlieferungen der Mitgliedstaaten als allgemeine Grundsätze des Gemeinschaftsrechts ergeben."

pflichteten Staaten völkerrechtlich verbindlich ist.[84] Die der Konvention beitretenden Staaten sind dazu verpflichtet, die Regelungen in innerstaatliches Recht umzusetzen. Andererseits formuliert die europäische Datenschutzkonvention die Grundprinzipien des europäischen Datenschutzes: die rechtmäßige Erhebung und Verarbeitung personenbezogener Daten nach Treu und Glauben (Art. 5 lit. a); die Zweckbindung der Datenerhebung und -verarbeitung (Art. 5 lit. b); den Verhältnismäßigkeitsgrundsatz bei der Erhebung und der Verarbeitung (Art. 5 lit. c); das Prinzip der Datenqualität (Art. 5 lit. d); Sonderregelungen zum Umgang mit sensiblen Daten (Art. 6); den Grundsatz der Datensicherheit (Art. 7); die Rechte des Betroffenen wie etwa das Auskunftsrecht sowie die Rechte auf Berichtigung und Löschung (Art. 8) sowie die grenzüberschreitende Übermittlung personenbezogener Daten zwischen Vertragsstaaten (Art. 12).

4. Die Europäische Union

Auch die Europäische Union gewährleistet den Datenschutz sowohl durch datenschutzrechtliche Regelungen im Rahmen der europäischen Grundrechte[85] als auch durch allgemeine und bereichsspezifische Datenschutzvorschriften. Während Art. 7 der EU-Charta in Anlehnung an die europäische Menschenrechtskonvention den Schutz des Privatlebens regelt, garantiert Art. 8 der EU-Charta als lex specialis zu Art. 7 der EU-Charta den Schutz personenbezogener Daten. Zu diesem Zweck hat die Europäische Union Richtlinien erlassen,[86] in denen die Mindeststandards für den Da-

84 European Treaty Series No. 108; EU, DS, EuRAT Con.

85 Der Charta der Grundrechte kam ursprünglich keine verbindliche Rechtswirkung zu; sie wird jedoch durch den Verweis in Artikel 6 des durch den Lissabonner Vertrag geänderten EU-Vertrages für alle Staaten – ausgenommen das Vereinigte Königreich und Polen – für bindend erklärt.

86 Beispielsweise (1) die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (RL 95/46/EG, ABl. EG 1995, L281, 31). Sie wurde am 25. Mai 2018 durch die am 4. Mai 2016 im Amtsblatt der Europäischen Union veröffentlichte Datenschutz-Grundverordnung (DSGVO) abgelöst. Die DSGVO ist eine Verordnung der Europäischen Union, mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht werden. Dadurch sollen zum einen der Schutz personenbezogener Daten innerhalb der Europäischen Union sichergestellt sowie zum anderen der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden. (2) Die Richtlinie über die Verarbeitung personenbezogener Daten und den

tenschutz beschrieben sind, die in allen Mitgliedstaaten der Europäischen Union durch nationale Gesetze sichergestellt werden sollen. Die Richtlinie 95/46/EG bildet zusammen mit der Konvention 108, der EU-Grundrechtecharta sowie der EMRK ein gemeinsames und umfassendes europäisches Datenschutzrecht.[87]

D. Freiheit vs. Sicherheit

Unter diesen veränderten gesellschaftlichen Bedingungen scheinen sowohl der Einzelne als auch die Gesellschaft in permanente Verunsicherung versetzt worden zu sein und zu Gunsten der Sicherheit willentlich seine bzw. ihre Freiheiten aufzugeben. Neue Bedrohungen wie Terroranschläge begünstigen die Tendenz, die Sicherheit *durch* den Staat gegenüber der Sicherheit *vor* dem Staat vorzuziehen. Im Zuge dieser Entwicklung wurden und werden weiterhin verschiedene neue technikgestützte Mittel sozialer Kontrolle eingeführt. Diese neuartigen Kontrollmittel sind deshalb fragwürdig, weil sie Eingriffe in die Grundrechte des Einzelnen, genauer gesagt, in seine Freiheit darstellen. Die gesellschaftlichen Veränderungen und die damit einhergehende zunehmend präventive Ausrichtung der staatlichen Sicherheitsvorsorge stellen das Verhältnis von Freiheit und Sicherheit vor neue Fragen. Der Staat muss auf der einen Seite die Grundrechte des Einzelnen berücksichtigen, ist auf der anderen Seite jedoch auch dazu verpflichtet, die notwendigen Maßnahmen zu ergreifen, um Sicherheit als eine Voraussetzung für Freiheit zu gewährleisten. Es handelt sich also um eine Kollision von Freiheit und Sicherheit, sodass sich zwei konfligierende Interessenkreise gegenüberstehen. Zu den Aufgaben des Gesetzgebers gehört es, zwischen diesen beiden Interessenkreisen einen Interessenausgleich herzustellen.

Freiheit und Sicherheit werden häufig als ein Gegensatzpaar begriffen. Sie stehen jedoch nicht in einem gegensätzlichen Verhältnis zueinander, sondern bedingen einander vielmehr wechselseitig.[88] Die Sicherheit soll grundsätzlich der Freiheit dienen. Der Staat übernimmt die doppelte Aufgabe der Gewährleistung von Freiheit und Sicherheit. Fraglich ist

---

Schutz der Privatsphäre in der elektronischen Kommunikation (RL 2002/58/EG, Abl. EG 2002, L201, 37).

87 *Genz*, Datenschutz in Europa und den USA, S. 19.

88 *Moser-Knierim*, Vorratsdatenspeicherung – Zwischen Überwachungsstaat und Terror-abwehr, S. 12.

dabei, ob die politischen Entscheidungen, die mit dem Slogan „Sicherheit vor Freiheit" bezeichnet werden können, verfassungskonform sind. Entscheidend ist demzufolge, wie der Staat diese doppelte Aufgabe verfassungskonform und optimal erfüllen kann. Als sich die Diskussion um das Folterverbot ausweitete, waren die deutschen Rechtswissenschaftler äußerst überrascht. Gleichwohl nimmt zurzeit die Tendenz zu, Freiheit für Sicherheit zu opfern. Die Notwendigkeit neuer Sozialkontrollmittel ist zu vergleichen mit der Notwendigkeit der Folter für die Rettung des Lebens. Beispielsweise werden bei der Vorratsdatenspeicherung als einer Art der oben beschriebenen neuen technikgestützten staatlichen Maßnahmen Telekommunikationsdaten durch einen Telekommunikationsdienstanbieter anlassunabhängig für einen bestimmten Zeitraum für Strafverfolgungs- und Gefahrenabwehrzwecke gespeichert. Damit wird die Möglichkeit eines staatlichen Zugriffs auf diese Daten zu einem späteren Zeitpunkt abgesichert. Dies kann insofern als ein beträchtlicher Angriff auf die Menschenwürde und als ein intensiver Eingriff in die Freiheit des Einzelnen betrachtet werden, als bei der Vorratsdatenspeicherung alle Bürger als potenzielle Täter gelten. Durch die Kombination verschiedener Daten können Persönlichkeitsprofile hergestellt und die Privatsphäre teilweise oder vollständig überwacht werden, und zwar im Namen der Sicherheitsgewährleistung für die Gesellschaft. Dies verursacht das Problem einer strategischen Abwägung zwischen Strafverfolgungseffizienz, Sicherheit und dem Schutz des Privaten. Somit sollte nach einem Modell gesucht werden, bei dem das gesellschaftliche Bedürfnis nach Sicherheit befriedigt und zugleich die Privatsphäre des Einzelnen geschützt werden können.

Im Zusammenhang damit behauptet *Isensee*, dass das Problem des Konflikts zwischen der Gewährleistung von Freiheit und Sicherheit mit einem „Grundrecht auf Sicherheit" gelöst werden soll.[89] Nach seiner Ansicht verpflichtet sich der Staat nicht nur dazu, die Grundrechte im Sinne des *status negativus* zu achten, sondern auch dazu, sie positiv zu schützen. Entgegen dem eindeutigen Wortlaut des Grundgesetzes konstruiert Isensee im Zusammenhang mit der Sicherheitsgewährleistung als der Grundlage von Freiheit ein Grundrecht auf Sicherheit als *status positivus* und definiert dieses als die Gesamtheit der Schutzpflichten des Staates.[90] Nach dieser Auffassung kommt diesem Grundrecht der Charakter eines

89 *Isensee*, Das Grundrecht auf Sicherheit, 1983.

90 *Comans*, Ein „modernes" europäisches Datenschutzrecht – Bestandsaufnahme und Analyse praktischer Probleme des europäischen Datenschutzes unter besonderer Berücksichtigung der Richtlinie zur Vorratsdatenspeicherung, S. 57.

Leistungsanspruchsrechts zu. Jedoch kann diese Konstruktion nicht dem Zweck dienen, dem Einzelnen einen Anspruch auf eine staatliche Leistung zuteilwerden zu lassen, sondern es geht darum, Eingriffe in das Freiheitsrecht, beispielsweise in das Recht auf informationelle Selbstbestimmung, zu legitimieren.[91] Angesichts des eigentlichen Charakters der Grundrechte als Abwehrrechte gegen den Staat ist es jedoch unhaltbar, aus den Grundrechten ein Grundrecht abzuleiten, das eine positive Handlung vom Staat fordert. Darüber hinaus droht die Gefahr, mit diesem Grundrecht staatliche Einschränkungen des Freiheitsrechts des Einzelnen ohne gewichtigen Grund zu legitimieren.

Angesichts des Umgangs mit den beträchtlichen Datenmengen, die bei der modernen Datenverarbeitung elektronisch gespeichert werden, können sich aus der Perspektive des Datenschutzes besondere Herausforderungen ergeben. Um unter diesem Gesichtspunkt betrachtet einem optimalen Interessenausgleich zwischen Freiheit und Sicherheit zu dienen, sollte zuerst geklärt werden, wie das Verfassungsrecht einer jeweiligen Gesellschaft Freiheit konstituiert und wie die Privatsphäre sowie die personenbezogenen Daten durch das Verfassungsrecht geschützt werden. Danach ist es erforderlich, konkrete Sicherheitsvorkehrungen zu analysieren, die zu diesem Schutz bei den einzelnen Maßnahmen, die zur Strafverfolgungseffizienz im modernen Staat klassisch oder neuartig eingesetzt werden, bereits zur Verfügung stehen. Aus diesem Grund soll im Folgenden auf die verfassungsrechtliche Grundlage in Bezug auf den Privatsphären- sowie Datenschutz eingegangen werden. Außerdem sollen drei neuartige Maßnahmen vorgestellt werden, aufgrund derer personenbezogene Daten verwertet werden dürfen. Durch die Analyse des Problems des Datenschutzes in diesen drei Bereichen soll das Kollisionsproblem zwischen Freiheit und Sicherheit bei der staatlichen Verwertung personenbezogener Daten hervorgehoben werden und es soll die Notwendigkeit des Ausgleichs zwischen Strafverfolgungseffizienz und Freiheitsgewährleistung durch Datenschutz betont werden.

Gegenwärtig steht die Gewährleistung von Freiheit und Sicherheit durch den Wandel gesellschaftlicher Bedingungen vor neuen Herausforderungen. Wie garantiert die Verfassung konkret den Schutz personenbezogener Daten? Welche Sicherheitsvorrichtungen verlangt die Verfassung für staatliche Maßnahmen, die personenbezogene Daten verwenden? Wie setzt die Verfassung dem Interesse der Ermittlungsbehörden, zu Sicherheitszwe-

91 *Kutscha*, in: *Roggan/Aden* (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, S. 31 m. w. N.

cken möglichst viele personenbezogene Daten der Bürger zu sammeln und zu verwenden, Grenzen? Wie sind diese Grenzen bei konkreten staatlichen Maßnahmen, die personenbezogene Daten verwenden, realisiert? Sind die bestehenden Grenzen hinreichend, um die Privatsphäre und die Daten zu schützen? Befinden sich der verfassungsrechtliche Schutz der Privatsphäre und der personenbezogenen Daten auf der einen und die Sicherheitsgewährleistung durch strafrechtliche Maßnahmen auf der anderen Seite im Zustand eines angemessenen Interessenausgleichs?

Um diese Fragen zu beantworten, ist es erforderlich, den verfassungsrechtlichen Schutz der Privatsphäre[92] und personenbezogener Daten konkret zu analysieren. Es geht darum, wie verfassungsrechtliche Vorgaben bei Sachverhalten konkretisiert sind. Anschließend sollen einige konkrete Maßnahmen als Beispiele für das Kollisionsverhältnis zwischen Freiheit und Sicherheit untersucht werden. Hierbei handelt es sich um das Strafregister, die Rasterfahndung und die Vorratsdatenspeicherung. Es soll untersucht werden, wie diese drei Maßnahmen gesetzlich ausgestaltet sind, inwiefern sie erfolgsversprechend sind – also ob sie für die Sicherheitsgewährleistung tatsächlich hilfreich sind – und welche Vorkehrungen getroffen wurden, um einen unbefugten oder unverhältnismäßigen Zugriff auf die im Strafverfahren verwendeten personenbezogenen Daten zu verhindern. Damit soll untersucht werden, ob die staatlichen Überwachungsmaßnahmen zu Sicherheitszwecken eine Gefährdung der verfassungsrechtlich garantierten Freiheiten darstellen und in welchem Umfang die Sicherheitspolitik in Freiheitsrechte eingreifen darf. Die hier durchgeführte rechtsvergleichende Untersuchung zu diesen Fragestellungen soll es ermöglichen, die Bedeutung, die der moderne Rechtsstaat der Privatsphäre und den personenbezogenen Daten beimisst, und damit das Schutzniveau der Privatsphäre und der personenbezogenen Daten zu erfassen. Aus den Ergebnissen dieser Untersuchung sollen Hinweise für einen angemessenen Interessenausgleich zwischen Freiheit und Sicherheit herausgearbeitet werden.

92 Der Begriff des Privatlebens ist ein auf Umstände bezogener Begriff, der sich mit Zeit, Ort und den sozialen und psychologischen Faktoren ändert. Er ist aber auch ein Mehrzweckkonzept, das in verschiedenen Umgebungen eine unterschiedliche Bedeutung hat. Es ist daher schwierig, den Begriff einheitlich zu definieren. In Deutschland ist unter der privaten Sphäre der Bereich einer Person zu verstehen, der nicht öffentlich ist, also der nur die eigene Person angeht. Durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG ist die Privatsphäre in besonderem Maße geschützt. Dieses Verständnis zeigt bereits die verschiedenen Auslegungsmöglichkeiten, die abhängig von zeitlichen oder örtlichen Verhältnissen bestehen.

Teil 2: Landesbericht Deutschland

A. Der verfassungsrechtliche Datenschutz

I. Privatsphären- und Datenschutz

1. Privatsphärenschutz

Sowohl auf nationaler als auch auf internationaler Ebene ist das Recht auf Privatsphäre i. w. S. anerkannt. Das deutsche Grundgesetz benennt allerdings kein spezielles Grundrecht auf den Schutz der Privatsphäre. Im deutschen Rechtsverständnis ist die Privatsphäre als ein nichtöffentlicher Bereich zu verstehen, in dem ein Mensch unbehelligt von äußeren Einflüssen sein Recht auf freie Entfaltung der Persönlichkeit wahrnimmt.[93] Die Privatsphäre des Einzelnen wird unter verschiedenen Aspekten und in Bereichen, die als Teile der Privatsphäre anzusehen sind, geschützt. Dem verfassungsrechtlichen Schutz der Privatsphäre dienen im Wesentlichen jene Rechte, die in Art. 2 Abs. 1, Art. 10 und Art. 13 GG niedergelegt sind.

Das Recht auf Unverletzlichkeit der Wohnung aus Art. 13 GG garantiert z. B. den Schutz der Integrität der Wohnung, die eine bedeutende Rolle im Privatsphärenschutz spielt. Dabei wird die Privatheit der Wohnung als „elementarer Lebensraum“[94] geschützt, der der freien Persönlichkeitsentfaltung des Einzelnen dient. In der eigenen Wohnung hat jedermann im Zusammenhang mit dem allgemeinen Persönlichkeitsrecht das Recht, in Ruhe gelassen zu werden, sodass staatliche Organe nicht gegen seinen Willen in den Wohnungsbereich eindringen oder darin verweilen dürfen.[95] Unter „Wohnung“ sind dabei die Räume zu verstehen, die der allgemeinen Zugänglichkeit durch eine räumliche Abschottung entzogen und zur Stätte privaten Lebens und Wirkens gemacht werden.[96] Ausreichend ist hierfür bereits ein vorübergehender Aufenthalt etwa in Hotel- oder Krankenzimmern, Campingwagen oder Zelten.[97] Unbebaute Flächen

93 BVerfGE 101, 361.
94 BVerfGE 42, 212 (219).
95 So bereits BVerfGE 51, 97 (107); BVerfGE 103, 142 (150 f.).
96 *Jarass*, Grundgesetz, Art. 13 Rn. 4.
97 *Epping*, Grundrechte, S. 342.

fallen dann in den Schutzbereich, wenn sie entweder gegenüber der Öffentlichkeit abgeschirmt sind oder wenn sie sich in unmittelbarer Nähe eines Gebäudes befinden und damit in erkennbarem Zusammenhang mit Wohnzwecken stehen.[98] Umstritten ist hingegen, ob auch Betriebs- und Geschäftsräume unter den Wohnungsbegriff zu subsumieren sind: Während in der Literatur mit Verweis auf den herkömmlichen Sprachgebrauch von „Wohnung" die Meinung verbreitet ist, dass Betriebs- und Geschäftsräume allein dem Schutz des Art. 2 Abs. 1 unterliegen,[99] und dass Betriebs- und Geschäftsräume nur dann als Wohnungen geschützt sind, wenn kein unkontrollierter öffentlicher Zutritt möglich ist,[100] werden solche Räume nach der Rechtsprechung uneingeschränkt von Art. 13 Abs. 1 geschützt.[101] Jedenfalls werden Betriebs- und Geschäftsräume, sei es als Wohnung oder als eine Grundlage der freien Persönlichkeitsentfaltung, als ein wichtiger Teil der Privatsphäre verfassungsrechtlich geschützt.

Der elementare Lebensraum wird zunächst gegen das unbegründete Eindringen oder Verweilen in einem Raum durch staatliche Organe gegen den Willen eines Einzelnen geschützt. Dementsprechend stellen Durchsuchungen von Wohnräumen – sei es zur Ergreifung von Tatverdächtigen (sog. Ergreifungsdurchsuchung) oder zum Auffinden von Beweismitteln (sog. Ermittlungsdurchsuchung) – laut Art. 13 Abs. 1 GG Eingriffe dar und unterliegen damit gemäß Abs. 2 dem Richtervorbehalt. Bei Gefahr im Verzug ist auch eine Anordnung durch die in den Gesetzen vorgesehenen anderen Organe möglich.

Die räumliche Privatsphäre wird auch vor technisch unterstützten Überwachungsmaßnahmen geschützt, selbst wenn diese von einem Bereich außerhalb der Wohnung ohne körperliches Betreten eingesetzt werden.[102] Diesen Schutz hat der technische Fortschritt in der modernen Gesellschaft erforderlich gemacht. Davon werden vor allem technische Mittel zur Überwachung von Wohnungen (sog. großer Lauschangriff)[103] erfasst. Im

98 *Kühne*, Grundgesetz, Art. 13 Rn. 3.

99 *Behr*, Vollstreckung ohne Durchsuchungsanordnung, NJW 1992, 2125, 2126; *Epping*, Grundrechte, S. 342.

100 *Ruthig*, Die Unverletzlichkeit der Wohnung (Art. 13 GG n. F.), JuS 1998, 506, 510.

101 BVerfGE 32, 54 (71 ff.).

102 Vgl. BVerfGE 109, 279 (309).

103 Mit der Einfügung der Abs. 3–6 wurden die verfassungsrechtlichen Grundlagen technischer Überwachungsmittel schon zuvor normierter und praktizierter Maßnahmen gelegt. Die Einfügung unterlag dabei der Kritik, die Grundgesetzänderung sei der Beginn der Einrichtung eines Überwachungsstaates. Zur nor-

Gegensatz zum großen Lauschangriff wird der kleine Lauschangriff eingesetzt, um einen in der Wohnung befindlichen Ermittler bzw. eine Vertrauensperson zu schützen. Durch diese Maßnahme werden Erkenntnisse darüber erlangt, was in der Wohnung geschieht. Diese Erkenntnisse hätte sich der in der Wohnung befindliche verdeckte Ermittler ohnehin angeeignet. Ausreichend ist eine Anordnung durch eine gesetzlich bestimmte Stelle. Es bedarf nur in dem Fall einer richterlichen Überprüfung, wenn die hierbei gewonnenen Informationen zum Zwecke der Strafverfolgung oder der Gefahrenabwehr verwertet werden sollen. Bei einer Gefahr im Verzug besteht eine Nachholmöglichkeit einer richterlichen Entscheidung. Hingegen werden durch den großen Lauschangriff Informationen über die Privatsphäre erlangt, die nicht im Beisein einer für die Polizei tätigen Person offenbart werden. Es werden dabei zweierlei Maßnahmen unterschieden. Einerseits handelt es sich um den repressiven Einsatz technischer Mittel – nur derjenigen, die der akustischen Überwachung dienen – zum Zweck der Strafverfolgung. Der Rechtfertigung repressiver akustischer Überwachung von Wohnungen sind spezielle Schranken gesetzt worden: Sie darf nur dann und nur auf Grund einer richterlichen Anordnung eingesetzt werden, wenn die Erforschung des Sachverhalts auf eine andere Weise unverhältnismäßig erschwert oder aussichtslos ist. Weiterhin ist die Maßnahme zeitlich zu befristen (Art. 13 Abs. 3 GG). Andererseits besteht bei präventiven Maßnahmen keine Beschränkung auf akustische Mittel. Optische Mittel wie Video- und Infrarotaufnahmen oder sonstige Mittel wie Peilsender sind demzufolge auch zulässig. Der kleine Lauschangriff ist also nur zur Abwehr einer dringenden Gefahr für die öffentliche Sicherheit zulässig. Um die Qualität der Begründetheit der Maßnahme zu gewinnen, bedarf sie einer richterlichen Anordnung, die bei Gefahr im Verzug auch nachgeholt werden kann.

Die Privatheit der Wohnung kann auch durch sonstige Maßnahmen wie das Betreten, Besichtigen oder Verweilen zu anderen Zwecken als der Durchsuchung beeinträchtigt werden. Die Wohnung als elementarer Lebensraum wird daher gegen Eingriffe und Beschränkungen i. S. d. Art. 13 Abs. 7 GG geschützt. Erforderlich ist dabei nicht das physische Eintreten, sondern der Einsatz technischer Mittel. Denn die Privatheit kann auch durch die Observation von außerhalb der Wohnung beeinträchtigt werden, beispielsweise, wenn der Betroffene sich „auf der Straße“ und

---

mativen Seite *Götz*, Allgemeines Polizei- und Ordnungsrecht, 12. Aufl., 1995, Rn. 520 f.; zur – nur lückenhaft verzeichneten – Praxis zuvor vgl. BT-Drs. 13/4942, S. 37 ff. Vgl. *Hermes*, Grundgesetz, Art. 13 Rn. 50 m. w. N.

damit außerhalb seiner Wohnung und dem hierdurch geschützten Bereich über sein Leben äußert, sodass diese Äußerungen von jedem mitgehört werden können.[104] Der Einsatz technischer Maßnahmen ist hierbei nur zur Abwehr einer gemeinen Gefahr oder einer Lebensgefahr für einzelne Personen, auf Grund eines Gesetzes auch zur Verhütung dringender Gefahren für die öffentliche Sicherheit und Ordnung, insbesondere zur Behebung der Raumnot, zur Bekämpfung von Seuchengefahr oder zum Schutze gefährdeter Jugendlicher zulässig.

Mit technischen Mitteln abgehörte und aufgezeichnete Gespräche innerhalb von Wohnräumen unterliegen ebenfalls dem grundrechtlichen Schutz nach Art. 13 Abs. 1 GG. Dieser Schutz erstreckt sich auf den Informations- und Datenverarbeitungsprozess, der sich an die Datenerhebung anschließt.[105] Werden erlangte Sachverhalte gespeichert und weiter genutzt, ist dieser Umgang mit personenbezogenen Daten auch an dem Grundrecht aus Art. 13 GG zu messen.[106]

Besonders kontrovers diskutiert wurde und wird in juristischen Kreisen die Grundrechtsrelevanz der verdeckten Online-Durchsuchung hinsichtlich des Wohnungsgrundrechts aus Art. 13 Abs. 1 GG. Bei Maßnahmen der Online-Durchsuchung handelt es sich um einen heimlichen Zugriff auf informationstechnische Systeme ohne physisches Betreten der Wohnung. Bei diesen liegt nach der Ansicht des Bundesverfassungsgerichts allein ein Eingriff in das Grundrecht auf Gewährleistung der Vertraulichkeit und der Integrität informationstechnischer Systeme vor.[107] Dazu werden weiter unten nähere Ausführungen vorgenommen.

Außerdem wird durch Art. 10 Abs. 1 GG das Brief-, Post- sowie Fernmeldegeheimnis geschützt. Der Artikel dient dem Schutz der Privatsphäre, damit die Kommunikation mit einem ortsabwesenden Partner, die durch die Vermittlung Dritter zustande kommt, vor einer mit dem Kommunikationsweg zusammenhängenden typischen Gefährdungslage geschützt wird, nämlich vor dem möglichen erleichterten Zugriff Dritter auf den Inhalt und die Umstände der Kommunikation.[108] Hierbei wird die freie

104 *Guttenberg*, Die heimliche Überwachung von Wohnungen – Zur verfassungsrechtlichen Problematik des § 9 II, III BVerfSchG und verwandter Vorschriften, NJW 1993, 567, 568 f.; *Jarass*, Grundgesetz, Art. 13 Rn. 8; *Ruthig*, Die Unverletzlichkeit der Wohnung (Art. 13 GG n. F.), JuS 1998, 506, 512.

105 *Tinnefeld*, in: *Tinnefeld/Buchner/Petri/Hof* (Hrsg.), Einführung in das Datenschutzrecht, S. 104.

106 Vgl. BVerfGE 109, 279 (326).

107 BVerfGE 120, 274 (274 ff.).

108 *Epping*, Grundrechte, S. 358.

Entfaltung der Persönlichkeit durch einen privaten, vor der Öffentlichkeit verborgenen Austausch von Informationen geschützt.

Das Briefgeheimnis erfasst Sendungen mit individueller schriftlicher Mitteilung sowie die mit der Briefsendung notwendigerweise anfallenden Daten wie Absender- und Empfängeradresse, Überbringer und Einzelheiten der Beförderung.[109] Demgegenüber werden vom Postgeheimnis alle postalisch beförderten Sendungen und die mit der Beförderung zusammenhängenden Daten unabhängig von einer individuellen Mitteilung geschützt.

Das Fernmeldegeheimnis, dem zurzeit eine erhebliche Bedeutung zukommt, schützt die Vertraulichkeit elektronisch vermittelter Kommunikation.[110] Dem grundrechtlichen Schutz unterliegen alle mittels Fernmeldetechnik ausgetauschten Informationen und die Kommunikationsumstände, die darüber Auskunft geben, „ob, wann, wie oft und zwischen welchen Personen oder Fernmeldeanschlüssen Telekommunikation erfolgte oder versucht wurde".[111] Damit fallen neben den Kommunikationsinhalten auch die näheren Umstände einer Kommunikation, nämlich solche Verbindungsdaten wie Ort, Zeit sowie Art und Weise der Kommunikation unter den Schutz des Fernmeldegeheimnisses. Vom Schutzbereich auszuschließen sind Rundfunkübertragungen oder Internetseiten, die an die Allgemeinheit oder an einen unbestimmten Personenkreis gerichtet sind,[112] sowie die nach Abschluss des Übertragungsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers gespeicherten Inhalte und Umstände der Kommunikation.[113] Es kommt dabei auf den Herrschaftsbereich des Kommunikationsteilnehmers an. Diese Schutzlücken in Bezug auf den Datenschutz können dank der Ergänzungsfunktion des allgemeinen Persönlichkeitsrechts zum Fernmeldegeheimnis gefüllt werden.

In das Grundrecht aus Art. 10 Abs. 1 GG kann dadurch eingegriffen werden, dass der Staat Kenntnis vom Inhalt der Kommunikation und den mit ihr zusammenhängenden Daten erlangt. Werden einmal durch einen Eingriff in das Grundrecht aus Art. 10 GG Daten erhoben, ist auch die spätere Verwendung dieser Daten an diesem Grundrecht zu messen.[114] Die Grundrechte binden direkt zwar ausschließlich die Gesetzgebung,

109 *Pagenkopf*, Grundgesetz, Art. 10 Rn. 12.
110 *Zippelius/Würtenberger*, Deutsches Staatsrecht, § 28 Rn. 2.
111 BVerfGE 67, 157 (172); BVerfGE 85, 386 (396).
112 *Pagenkopf*, Grundgesetz, Art. 10 Rn. 14a; *Hermes*, Grundgesetz, Art. 10 Rn. 28; *Jarass*, Grundgesetz, Art. 10 Rn. 4.
113 BVerfGE 115, 166 (166).
114 BVerfGE 125, 260 (313).

die vollziehende Gewalt und die Rechtsprechung, jedoch kommen sie indirekt auch für die Regelung der Beteiligung nichtöffentlicher Stellen an Telekommunikationsdiensten zur Geltung, weil § 88 TKG jeden Dienstanbieter zur Wahrung des Fernmeldegeheimnisses verpflichtet und darüber hinaus der Staat aufgrund der staatlichen Schutzpflichten dafür Sorge zu tragen hat, dass die privaten Dienstleister die Vertraulichkeit der Kommunikation ebenso gewährleisten wie die staatliche Post.[115] Das Fernmeldegeheimnis schützt demzufolge den einzelnen Bürger nicht nur vor der Kenntnisnahme von Telekommunikationsinhalten durch staatliche Stellen, sondern auch davor, dass öffentliche Stellen die Telekommunikation der Kenntnisnahme Dritter aussetzen. Bei einem derartigen mittelbaren Eingriff in das Fernmeldegeheimnis durch die Veranlassung Dritter zur Kenntnisnahme fremder Telekommunikation in der Übermittlungsphase kann der Schutzanspruch geltend gemacht werden.

Beschränkungen dieses Grundrechts bedürfen gemäß Art. 10 Abs. 2 S. 1 GG einer gesetzlichen Grundlage. Anders als bei der Unverletzlichkeit der Wohnung aus Art. 13 GG enthält dieses Grundrecht keinen Richtervorbehalt. Da Eingriffe in das Grundrecht aus Art. 10 Abs. 1 GG zumeist heimlich erfolgen, kann die Gewährleistung effektiven Rechtsschutzes allerdings einen Richtervorbehalt erforderlich machen.[116] In der Regel findet sich ein solcher zwar in den einschränkenden Gesetzen wie z. B. in § 100b StPO, jedoch scheint das auch deshalb noch problematisch zu sein, da der Richtervorbehalt in der Praxis nur eingeschränkt funktioniert: Nach einer Studie von *Backes* und *Gusy*[117] wurde lediglich bei einem Viertel der Anträge auf Telefonüberwachung eine dem Gesetz entsprechende richterliche Prüfung durchgeführt. Nach Art. 10 Abs. 2 S. 2 GG ist es möglich, bei Beschränkungen zum Zweck des Schutzes der freiheitlich demokratischen Grundordnung auf die Mitteilung an den Betroffenen zu verzichten und sie stattdessen durch die Information eines von der Volksvertretung bestimmten Organs bzw. Hilfsorgans zu ersetzen. Daraus kann geschlossen werden, dass die Betroffenen bei Eingriffen in das Grundrecht aus Art. 10 Abs. 1 GG zum effektiven Rechtsschutz zu benachrichtigen sind. Da eine richterliche Überprüfung der Maßnahme demgegenüber ohne eine Mitteilung an den Betroffenen unmöglich gemacht wird, wurden in der Literatur im Hinblick auf die Menschenwürde, das Rechtsstaatsprinzip und

115 BVerfGE 106, 28 (37).
116 BVerfGE 125, 260 (337 ff.).
117 *Backes/Gusy*, Wer kontrolliert die Telefonüberwachung? – Eine empirische Untersuchung zum Richtervorbehalt bei der Telefonüberwachung, 2003, S. 44.

die Gewaltenteilung Bedenken gegen die Verfassungsmäßigkeit des Art. 10 Abs. 2 S. 2 GG angemeldet, denen jedoch das Bundesverfassungsgericht entgegengetreten ist.[118]

Das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG gewährt außerdem den Schutz eines wesentlichen, unantastbaren Bereichs privater Lebensgestaltung. Es wurde im Rahmen der Zivilrechtsprechung in der „Leserbrief-Entscheidung"[119] des Bundesgerichtshofs erstmals als ein verfassungsmäßig gewährleistetes Grundrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1[120] abgeleitet und der Schutz vor dem Eingriff in die Privatsphäre des Einzelnen wurde als wesentlicher Bestandteil des verfassungsrechtlichen Persönlichkeitsschutzes definiert.[121] In seiner Ausprägung als Schutz der Privatsphäre gewährleistet das allgemeine Persönlichkeitsrecht für den Einzelnen die Existenz eines räumlich und thematisch bestimmten Bereichs, der grundsätzlich frei von unerwünschter staatlicher Einsichtnahme bleiben soll.[122] Das Bundesverfassungsgericht hebt gegenüber dem „aktiven" Element der freien Entfaltung der Persönlichkeit – der allgemeinen Handlungsfreiheit – das Recht auf Respektierung der Privatsphäre und des sozialen Geltungsanspruchs des Einzelnen hervor.[123] Aufgabe des allgemeinen Persönlichkeitsrechts sei es, „die engere persönliche Lebenssphäre und die Erhaltung ihrer Grundbedingungen zu gewährleisten, die sich durch die traditionellen konkreten Freiheitsgarantien nicht abschließend erfassen lassen".[124] Das Bundesverfassungsgericht trägt damit den vielfältigen Ausprägungen des allgemeinen Persönlichkeitsrechts im Sinne der Sphärentheorie Rechnung, nach der zwischen der Intimsphäre, der Privatsphäre und der Sozialsphäre zu unterscheiden ist. Diese Differenzierung ist deswegen von Bedeutung, weil sich die Anforderungen, die an eine Eingriffsrechtfertigung zu stellen sind, danach richten, welche Lebenssphäre berührt ist. Beispielsweise darf in die

118 BVerfGE 30, 1 (1 ff.); vgl. *Jarass*, Grundgesetz, Art. 10 Rn. 20.
119 BGHZ 13, 334 (334 ff.).
120 Die Verbindung von Art. 1 Abs. 1 und Art. 2 Abs. 1 bedeutet nicht, dass hier zwei Grundrechte kumulativ zur Anwendung kämen. Aus dieser Verbindung ergibt sich vielmehr eine Verstärkung des Schutzes (*Murswiek/Rixen*, Grundgesetz, Art. 2 Rn. 63).
121 *Degenhart*, Das allgemeine Persönlichkeitsrecht, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, JuS 1992, 362.
122 BVerfGE 120, 274 (311); vgl. auch BVerfGE 27, 344 (350 ff.); BVerfGE 44, 353 (372 f.); BVerfGE 90, 255 (260); BVerfGE 101, 361 (382 f.).
123 BVerfGE 54, 148 (153 f.).
124 BVerfGE 54, 148 (153).

Intimsphäre als einen Bereich der totalen Zurückgezogenheit auf keinen Fall eingegriffen werden. In die Privatsphäre soll hingegen zwar eingegriffen werden können, allerdings nur unter besonders strenger Wahrung des Verhältnismäßigkeitsgrundsatzes, während Eingriffe in die Sozialsphäre unter „normalen" Kriterien als Eingriffe in die Handlungsfreiheit gerechtfertigt werden können.

Der Schutzbereich des allgemeinen Persönlichkeitsrechts ist relativ offen. Damit das allgemeine Persönlichkeitsrecht die Entwicklungsoffenheit gewinnt, wird dessen Schutzbereich von der Rechtsprechung nicht abschließend definiert.[125] Damit können neue, bisher unbenannte Ausprägungen des allgemeinen Persönlichkeitsrechts, die zum gegenwärtigen Zeitpunkt noch nicht ersichtlich sind, geschützt werden. Dadurch kann das allgemeine Persönlichkeitsrecht mit neuartigen Gefährdungen der Persönlichkeitsentfaltung Schritt halten, wie sie insbesondere vom wissenschaftlich-technischen Fortschritt ausgehen.[126] Dies ist vor allem im Bereich des Datenschutzes von Bedeutung. Im Hinblick auf die Entwicklung moderner Kommunikations- und Informationstechnologien sowie mit Blick auf vorhandene EDV-Bedingungen trägt das allgemeine Persönlichkeitsrecht als eine Grundlage der Gewährleistung der allgemeinen Freiheit maßgeblich zu einer umfassenden sowie effektiven Sicherung des Persönlichkeitsschutzes im digitalen Zeitalter bei.

In diesem Zusammenhang sind vom Bundesverfassungsgericht bestimmte Ausprägungen des allgemeinen Persönlichkeitsrechts entwickelt worden: das Recht auf sexuelle Selbstbestimmung, das Recht auf individuelle Selbstbestimmung, das Recht auf wirtschaftliche Selbstbestimmung, das Recht am eigenen Wort, das Recht auf Selbstdarstellung, gar das Recht an der eigenen Wohnung und das Recht an eigenen Daten.[127]

Das allgemeine Persönlichkeitsrecht wird jedoch nicht uneingeschränkt gewährleistet. Es unterliegt der Schrankentrias der Rechte Anderer, der verfassungsmäßigen Ordnung und des Sittengesetzes. Die Schranken des Art. 2 Abs. 1 sind allerdings keine verfassungsunmittelbaren Freiheitseinschränkungen, sondern sie ermächtigen den Gesetzgeber, Freiheitseinschränkungen vorzunehmen. Eingriffe der öffentlichen Gewalt sind daher

125 *Weidner-Braun*, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung – am Beispiel des personenbezogenen Datenverkehrs im www nach deutschem öffentlichen Recht, S. 76.

126 *Murswiek/Rixen*, Grundgesetz, Art. 2 Rn. 66.

127 Vgl. *Ehmann*, Zur Struktur des Allgemeinen Persönlichkeitsrechts, JuS 1997, 193, 197.

nur auf Grundlage eines hinreichend bestimmten und verhältnismäßigen Gesetzes zulässig.[128]

2. Die Bedeutung des Datenschutzes für den Privatsphärenschutz

Genau wie das Recht auf den Privatsphärenschutz ist auch *das Recht auf Datenschutz* im Grundgesetz nicht ausdrücklich genannt. Als die öffentliche Verwaltung damit begann, personenbezogene Daten zunehmend automatisiert zu verarbeiten, entstand die Möglichkeit, personenbezogene Daten schnell miteinander zu verknüpfen, zu übermitteln und in neue Sachzusammenhänge zu stellen. Damit einhergehend erhöhte sich die Furcht vor der Möglichkeit der aus den Entwicklungen der Informationstechnik resultierenden Persönlichkeitsgefährdungen und vor einem gänzlich erfassten, „gläsernen" Einzelnen, der unsichtbar und unkontrolliert gesteuert werden kann. Das Bundesverfassungsgericht hat infolgedessen mit seinem Volkszählungsurteil[129] vom 15. Dezember 1983 das Recht auf informationelle Selbstbestimmung[130] als einem weiteren spezifischen Aspekt der Privatsphäre und elementaren Teil des allgemeinen Persönlichkeitsrechts aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 abgeleitet.[131] Damit hat das Bundesverfassungsgericht nicht nur das allgemeine Persönlichkeitsrecht präzisiert, sondern aus diesem *ein Grundrecht auf Datenschutz* herausgearbeitet.

Wie bereits dargelegt, lässt sich im Grundgesetz zwar kein ausdrückliches Grundrecht auf Privatsphäre finden, jedoch werden mehrere Aspekte der Privatsphäre verfassungsrechtlich gewährleistet, um die Privatsphäre als Grundbedingung der freien Entfaltung der Persönlichkeit zu schützen. Dabei spielen Art. 13 und Art. 10 GG eine bedeutende Rolle. Während

128 *Weidner-Braun*, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung – am Beispiel des personenbezogenen Datenverkehrs im www nach deutschem öffentlichen Recht, S. 75.

129 Im Volkszählungsurteil geht es um die Verfassungskonformität der im VoZählG im Jahre 1983 vorgesehenen Datenerhebungsregelungen für statistische Zwecke und Übermittlungsregelungen.

130 Der Ausdruck „das Recht auf informationelle Selbstbestimmung" wurde erstmals im Jahre 1971 von Steinmüller genutzt, wobei er das Recht auf informationelle Selbstbestimmung in dem Sinne erfasste, dass der Einzelne selbst darüber bestimmt, unter welchen Umständen er welche personenbezogenen Daten an wen übermittelt (*Steinmüller*, Grundfragen des Datenschutzes: Gutachten im Auftrag des Bundesministeriums des Innern, Deutscher Bundestag – 6. Wahlperiode – BT-Drs. 6/3826 Anlage I, 1971.

131 BVerfGE 65, 1 (41 ff.).

Art. 13 die Unverletzlichkeit der Wohnung als einen räumlichen elementaren Lebensraum schützt, dient Art. 10 dem Schutz eines privaten, vor der Öffentlichkeit verborgenen Austausches von Informationen. Außerdem kann das allgemeine Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m Art. 1 Abs. 1 GG die Füllmasse der durch die beiden Grundrechte entstandenen Schutzlücken bieten. Daraus leitet das Bundesverfassungsgericht die konkreten Ausprägungen um des Schutzes der Privatsphäre willen ab und bewältigt zugleich mit der Sphärentheorie das Problem von Eingriffen in das allgemeine Persönlichkeitsrecht. Es entsteht demnach die Intimsphäre, die vollständig vor staatlichen Eingriffen geschützt wird und in die ein Eingriff daher in keinem Fall gerechtfertigt werden kann. In die Privatsphäre und die Sozialsphäre darf hingegen eingegriffen werden, allerdings nur unter verschiedenen Voraussetzungen zur Rechtfertigung, abhängig davon, welche Lebenssphäre berührt wird. Für einen Eingriff in die Privatsphäre wird eine strengere Wahrung des Verhältnismäßigkeitsgrundsatzes als für den Eingriff in die Sozialsphäre gefordert.

Im Hinblick auf den Datenschutz hat das Bundesverfassungsgericht zwei Grundrechte aus dem allgemeinen Persönlichkeitsrecht entwickelt: das Recht auf informationelle Selbstbestimmung sowie das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme. Unter den modernen Bedingungen der Datenverarbeitung kommt dem Recht auf informationelle Selbstbestimmung eine erhebliche Bedeutung zu. Es schützt den Einzelnen vor einzelnen, punktuellen Datenerhebungen mit personenbezogenem Inhalt und den sich der Datengewinnung anschließenden Interpretationsmöglichkeiten.[132] Demgegenüber wird bezweifelt, ob das IT-Grundrecht, welches das Bundesverfassungsgericht mit Bezug auf Online-Durchsuchungen neu geschaffen hat, erforderlich ist bzw. ob es überhaupt dem effektiveren Schutz der Privatsphäre dient.

3. Der verfassungsrechtliche Datenschutz

Die personenbezogenen Daten, denen beim Privatsphärenschutz eine große Bedeutung zukommt, werden auch verfassungsrechtlich geschützt. Für

132 Ausführlich zu dem Recht auf Datenschutz, *Poscher*, The Right to Data Protection – A No-Right Thesis, in: *Miller*, Privacy and Power – a Transatlantic Dialogue in the Shadow of the NSA-Affair, S. 129–142, Cambridge University Press, 2017.

deren Schutz hat das Bundesverfassungsgericht ein besonderes Grundrecht aus dem allgemeinen Persönlichkeitsrecht abgeleitet: das Recht auf informationelle Selbstbestimmung. Das Grundrecht dient dem Privatsphären- und insbesondere dem Datenschutz.

Das Recht auf informationelle Selbstbestimmung gibt dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen.[133] Personenbezogene Daten sind gemäß § 27 Abs. 3 BDSG angelehnt an „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person".[134] Das Recht auf informationelle Selbstbestimmung geht über den Schutz der Privatsphäre hinaus, da es den Schutz bereits auf der Stufe der Persönlichkeitsgefährdung in Kraft treten lässt.[135] Es schützt also vor einzelnen, punktuellen Datenerhebungen mit personenbezogenem Inhalt und den sich der Datengewinnung anschließenden Interpretationsmöglichkeiten.[136]

Unter den Bedingungen der modernen Datenverarbeitung setzt die freie Entfaltung der Persönlichkeit voraus, dass der Einzelne vor unbegrenzter Erhebung, Speicherung, Verwendung und Weitergabe seiner personenbezogenen Daten geschützt wird.[137] Es ist für den einzelnen Bürger jedoch schwierig, Kenntnis davon zu haben, welche Daten gesammelt werden, wo sie erhoben werden, ob sie gespeichert werden und was mit diesen Daten geschieht. Menschen, die denken, dass ihre Daten systematisch identifiziert und überwacht werden, verzichten wahrscheinlich darauf, ihre Rechte auszuüben und sich der Öffentlichkeit zu stellen, weil sie fürchten, dass sie durch diese Aktivitäten benachteiligt werden. In diesem Zusammenhang hat das Bundesverfassungsgericht mit seinem Volkszählungsurteil vom 15. Dezember 1983 die Notwendigkeit eines besonderen Maßes an Schutz des Rechts auf informationelle Selbstbestimmung unter den damaligen, heutigen und künftigen Bedingungen der automatischen Datenverarbeitung anerkannt. Denn die personenbezogenen Daten seien laut Bundesverfassungsgericht heute mit Hilfe der automatischen Datenverarbeitung technisch gesehen unbegrenzt speicherbar und jederzeit ohne Rücksicht auf Entfernungen in Sekundenschnelle abrufbar. Das Bundesverfassungsgericht befürchtet außerdem, dass personenbezogene Daten oh-

133 BVerfGE 120, 274 (312); BVerfGE 65, 1 (43).
134 BVerfGE 65, 1 (42).
135 BVerfGE 120, 274 (311 f.).
136 *Kingreen/Poscher*, Grundrechte Staatsrecht II, S. 120 f.
137 BVerfGE 65, 1.

ne die zureichende Kontrollmöglichkeit des Betroffenen im Hinblick auf Richtigkeit und Verwendung seiner Daten mit anderen Datensammlungen zu einem teilweise oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden.[138] Das Bundesverfassungsgericht spricht hier von einer gewaltigen Bedrohung für die Ausübung der Freiheitsrechte.

Mit der Ableitung dieses Rechts aus dem allgemeinen Persönlichkeitsrecht zielt das Bundesverfassungsgericht darauf ab, den neuen Gefährdungen durch die automatisierte Datenverarbeitung wirksam entgegenzutreten. Nach der Rechtsprechung wird in das Recht nur unter den folgenden Voraussetzungen eingegriffen:

1. Ein Eingriff in das Recht bedarf einer verfassungsgemäßen gesetzlichen Grundlage;
2. Die gesetzliche Grundlage muss so normenklar bestimmt werden, dass der Einzelne die Voraussetzungen und den Umfang des Eingriffs klar erkennen kann (Normenklarheitsgebot);
3. Die Eingriffsnorm muss dem Verhältnismäßigkeitsgrundsatz entsprechen;
4. Der Verwendungszweck muss im Voraus festgelegt werden und hinreichend bestimmt sein (Zweckbindungsgrundsatz);
5. Es bedarf organisatorischer und verfahrensrechtlicher Vorkehrungen zur Sicherung des Rechts auf informationelle Selbstbestimmung. Zu diesen Vorkehrungen zählen die Transparenz der Datenvorgänge durch Aufklärung des Betroffenen, eine dem Betroffenen zur Verfügung gestellte Auskunft und Sperrung bzw. Löschung seiner Daten zum gegebenen Zeitpunkt sowie die Einrichtung und Beteiligung von Datenschutzinstanzen, die rechtlich unabhängig und faktisch dazu befähigt sind, über die Rechte der Bürger zu wachen.

Die Bedeutung dieses Urteils besteht darin, dass damit einheitliche Grundsätze als Prüfungsmaßstab für jeden Eingriff in personenbezogene Daten, unabhängig von ihrer Sensibilität,[139]geschaffen wurden. Denn es gibt unter modernen Bedingungen der automatisierten Datenverarbeitung kein belangloses Datum mehr.[140]

---

138 BVerfGE 65, 1 (42).

139 BVerfGE 65, 1 (44 f.): Nach der Rechtsprechung gebe es unter den Bedingungen der automatisierten Datenverarbeitung wegen der der Informationstechnologie inhärenten Verarbeitungs- und Verknüpfungsmöglichkeiten „kein belangloses Datum“ mehr.

140 BVerfGE 65, 1 (45).

Dennoch kommt das Recht auf informationelle Selbstbestimmung als Konkretisierung des Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG nicht zur Anwendung, wenn speziellere Grundrechte betroffen sind. Speziellere Grundrechte verdrängen also in ihrem Anwendungsbereich das Recht auf informationelle Selbstbestimmung bzw. das allgemeine Persönlichkeitsrecht. Sofern laufende Kommunikationsvorgänge betroffen sind, wird Art. 10 Abs. 1 GG angewendet. In das Recht auf informationelle Selbstbestimmung darf erst dann eingegriffen werden, wenn die Telekommunikation abgeschlossen und die Daten endgültig auf einem Speichersystem gespeichert sind.[141]

Das Bundesverfassungsgericht hat mit seinem Online-Durchsuchungsurteil vom 27. Februar 2008 neben dem Recht auf informationelle Selbstbestimmung auch ein verfassungsrechtlich neues Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als eine weitere Ausprägung des allgemeinen Persönlichkeitsrechts entwickelt.[142] Das Grundrecht ist subsidiär zu dem Recht auf informationelle Selbstbestimmung.[143] Bei der Online-Durchsuchung greifen staatliche Organe ohne Beschlagnahmung des Geräts auf die Daten eines Computers zu. Stattdessen erfolgt der Zugriff dadurch, dass unbemerkt eine staatliche Überwachungssoftware auf dem Computer installiert wird. Anders als beim informationellen Selbstbestimmungsrecht, dessen Schutzgegenstand die Entscheidungsfreiheit des Einzelnen über seine persönlichen Daten ist, werden bei diesem Grundrecht die informationstechnischen Systeme selbst geschützt.

Das neue „IT-Grundrecht", das das Bundesverfassungsgericht in seinem Urteil vom 27. Februar 2008 erstmals als Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme explizit benannte,[144] begründet sich darin, dass die Gewährleistung der Grundrechte aus Art. 10 und Art. 13 GG sowie die vom Bundesverfassungsgericht bisher entwickelten Ausprägungen des allgemeinen Persönlichkeitsrechts dem Bedürfnis des Schutzes vor den Persönlichkeitsgefährdungen, die sich

141 BVerfGE 110, 33 (53); *Gercke*, Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit, CR 2007, 245, 251.

142 BVerfGE 120, 274.

143 Das „neue" Grundrecht begrüßend: *Hömig*, „Neues" Grundrecht, neue Fragen?, Zum Urteil des BVerfG zur Online-Durchsuchung, Jura 2009, 207, 213; siehe auch sehr kritisch zur Erforderlichkeit der eigenständigen Existenz des Grundrechts: *Eifert*, Informationelle Selbstbestimmung im Internet, NVwZ 2008, 521, 521 ff.

144 BVerfGE 120, 274 (302).

aus der Entwicklung der Informationstechnik ergeben, nicht hinreichend Rechnung tragen.[145] Das Grundrecht schließt die Lücke im Grundrechtsschutz, die für eine solche Infiltration des gesamten informationstechnischen Systems besteht, das außerhalb einer Wohnung steht, und für solche Daten, die nach Abschluss eines Kommunikationsprozesses nicht mehr von Art. 10 Abs. 1 GG gedeckt sind und mangels einzelner punktueller Datenerhebung auch nicht oder nicht ausreichend dem Recht auf informationelle Selbstbestimmung unterliegen.[146,147]

Nach der Entscheidung des Bundesverfassungsgerichts ist der Schutzbereich von Art. 13 Abs. 1 GG im Falle von Online-Durchsuchungen nicht betroffen. Dafür sprechen einige Argumente: Online-Durchsuchungen würden die räumliche Sphäre der Wohnung als geschütztem Rückzugsraum nicht beeinträchtigen, weil sie sich rechtlich und tatsächlich ausschließlich auf eine dem Betroffenen gehörende Sache beschränken.[148] Ein raumbezogener Schutz sei nicht in der Lage, die spezifische Gefährdung des informationstechnischen Systems abzuwehren.[149] Da informationstechnische Systeme oft mobil sind und daher sowohl innerhalb als auch außerhalb einer Wohnung im Sinne von Art. 13 GG betrieben werden können, halten einige Autoren das Wohnungsgrundrecht für nicht anwendbar.[150] Die Betroffenheit des Schutzbereichs wird also verneint, weil der Staat bei einer Online-Durchsuchung lediglich Einsicht in einen

145 BVerfGE 120, 274 (306).

146 *Horn*, Grundrechte, Art. 2 Rn. 51.

147 Vgl. *Hoffmann-Riem*, Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, 1009, 1016. Erst die sich an die Infiltration anschließende Datenauswertung fällt wieder unter das Recht auf informationelle Selbstbestimmung.

148 BGH, Ermittlungsrichter, StV 2007, 60 (62); *Gercke*, Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit, CR 2007, 245, 250; *Hoffmann*, Die Online-Durchsuchung: staatliches Hacken oder zulässige Ermittlungsmaßnahme?, NStZ 2005, 121, 124.

149 BVerfGE 120, 274 (310); zustimmend *Bär*, Anmerkung zum Urteil des BVerfG: Verfassungsmäßigkeit der Online-Durchsuchung und anderer verdeckter Ermittlungsmaßnahmen in Datennetzen, MMR 2008, 325, 325.

150 *Böckenförde*, Grundrechtstheorie und Grundrechtsinterpretation, in: *ders.*, Staat, Gesellschaft, Freiheit. Studien zur Staatstheorie und zum Verfassungsrecht, S. 223 f.; *Lepsius*, Das Computer-Grundrecht: Herleitung – Funktion – Überzeugungskraft, in: *Roggan* (Hrsg.), Online-Durchsuchung – Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar 2008, 2008, 21, 25: Es mute merkwürdig an, wenn der Grundrechtsschutz davon abhinge, ob der Nutzer informationstechnischer Systeme auf diese innerhalb oder außerhalb der Wohnung zugreife.

begrenzten Teil der Wohnung habe und somit dem Betroffenen noch Raum bleibe, den er als privaten Rückzugsort nutzen könne.[151] Schließlich wird die Schutzbereichseröffnung mit dem Hinweis darauf verneint, dass Online-Durchsuchungen ohne die Überwindung physischer Barrieren vorgenommen werden können.[152] Da das Fernmeldegeheimnis nicht auf den Schutz von Daten abzielt, die sich nach Abschluss eines Kommunikationsvorgangs im Herrschaftsbereich des Kommunikationsteilnehmers befinden,[153] ist Art. 10 GG nicht einschlägig. Schlussendlich sieht das Bundesverfassungsgericht auch das Recht auf informationelle Selbstbestimmung nicht als einschlägig an, da es dabei nicht um die Erhebung einzelner Daten gehe, sondern um einen Datenbestand, der Einblicke in wesentliche Teile der Lebensgestaltung ermögliche.[154]

Jedoch ist die Argumentation, nach der Online-Durchsuchungen keine Beeinträchtigung der räumlichen Sphäre, sondern nur eine begrenzte Einsicht in die Wohnung darstellen würden, nicht überzeugend. Das Wohnungsgrundrecht gewährt grundsätzlich einen Ort, an dem sich jeder Einzelne ohne staatliche Einsichtnahmen frei entfalten kann. Geschützt werden konsequenterweise alle Vorgänge und auch alle Gegenstände, soweit sie innerhalb der Wohnung geschehen bzw. sich darin befinden. Die Unmöglichkeit der umfassenden Schutzgewährleistung des Wohnungsgrundrechts läuft auch nicht notwendigerweise darauf hinaus, dass die Nutzung informationstechnischer Systeme niemals in den Schutzbereich des Wohnungsgrundrechts fallen würde. Auch ein wechselnder Standort verhindert nicht die Schutzbereichseröffnung. Gerade der Umstand, dass ein und dieselbe Handlung je nach ihrem Standort vom Wohnungsgrundrecht geschützt ist oder nicht, ist das Wesensmerkmal eines raumbezogenen Schutzes.[155] Wie bei der Ablehnung der Schutzbereichseröffnung des Art. 13 GG ist auch die Begründung der Anerkennung von Schutzlücken des Rechts auf informationelle Selbstbestimmung nicht überzeugend. Denn

151 So *Schlegel*, Warum die Festplatte keine Wohnung ist – Art 13 GG und die „Online-Durchsuchung", GA 2007, 648, 659; ähnlich wohl auch *Gercke*, Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit, CR 2007, 245, 250.

152 *Gercke*, Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit, CR 2007, 245, 250: Nach seiner Meinung sei die Situation vergleichbar mit dem Blick eines Ermittlungsbeamten durch ein Fenster. Niemand würde dies als eine Wohnraumüberwachung qualifizieren.

153 BVerfGE 120, 274 (307 f.).

154 BVerfGE 120, 274 (312 f.).

155 *Schneider*, Rechtliche Rahmenbedingungen für die Vornahme von Online-Durchsuchungen, S. 54.

das Recht auf informationelle Selbstbestimmung ist auf keinen Fall auf die Erhebung eines einzelnen Datums beschränkt.[156] Nicht ersichtlich ist, aus welchem Grund man einen Unterschied zwischen der Behandlung einer einzelnen Datenabfrage und der Erhebung ganzer Datenbestände verbunden mit der Potenzierung der Gefährdung der Persönlichkeitsrechte machen sollte. In diesem Zusammenhang wird bezweifelt, ob neben der Unverletzlichkeit der Wohnung und dem Recht auf informationelle Selbstbestimmung die weitere Schaffung des *neuen* Grundrechts um des besonderen Schutzes der Freiheit der Bürger willen effektiver oder sogar überhaupt erforderlich ist. Denn den gesteigerten Gefahren für das Persönlichkeitsrecht des Einzelnen infolge der technischen Entwicklung könnte mit dem strengeren Verhältnismäßigkeitsgrundsatz begegnet werden: An den verfolgten Zweck sind umso höhere Anforderungen zu stellen, je stärker in den Bereich privater Lebensgestaltung eingegriffen wird. Darüber hinaus könnten diese neuen Herausforderungen auch nur mit dem Schutz des absolut geschützten Kernbereichs, den konkreten Gefährdungsdelikten vor der Rechtsgutsverletzung, der Beachtung der Normklarheit sowie -bestimmtheit und den verfahrensrechtlichen Voraussetzungen überwunden werden.

Das Bundesverfassungsgericht hat insoweit besondere Anforderungen an die Rechtfertigung von Eingriffen mit hoher Intensität gestellt, nämlich gesteigerte Anforderungen an die mit dem Eingriff verfolgten Ziele sowie an die Sicherstellung verfahrensrechtlicher Vorkehrungen. Weiterhin ist der Betroffene auch nachträglich über die Möglichkeit des Rechtsschutzes zu benachrichtigen.[157]

II. Übersicht des einfachgesetzlichen Datenschutzsystems

Im Jahr 1977 erließ die Bundesrepublik Deutschland die erste Fassung des Bundesdatenschutzgesetzes (BDSG). Nach dem Volkszählungsurteil des Bundesverfassungsgerichts im Jahre 1983 war klar, dass das bisherige Datenschutzgesetz den verfassungsrechtlichen Anforderungen nicht genügte. Das Gesetz musste also einige Novellierungen erfahren. Entsprechend den im Volkszählungsurteil des Bundesverfassungsgerichts genannten Anforderungen wurde das BDSG vor allem im Jahre 1990 novelliert.

156 *Epping*, Grundrechte, S. 328.
157 BVerfGE 120, 274 (323 ff.).

Das BDSG regelt die Datenerhebung, -verarbeitung und -nutzung. Ein Erheben im Sinne des Gesetzes liegt bei der bloßen Beschaffung von Daten über natürliche Personen beim Betroffenen oder bei Dritten vor. Zur Verarbeitung gehören das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Unter einer Nutzung ist jede Verwendung personenbezogener Daten zu verstehen, soweit es sich nicht um die Verarbeitung handelt. Im BDSG wird zwar zwischen dem Datenschutz in öffentlichen und nichtöffentlichen Stellen unterschieden, es regelt jedoch den Datenschutz in beiden Bereichen.

Wird das deutsche Datenschutzrechtssystem übersichtlich vorgestellt, können zwei Besonderheiten festgestellt werden. Die erste betrifft den Datenschutzansatz. Das deutsche Datenschutzrecht folgt einem umfassenden Ansatz. Es gibt ein umfassendes Datenschutzgesetz (BDSG), in dem alle Datenverarbeitungsvorgänge im öffentlichen und privaten Sektor reguliert werden. Zweitens ist im BDSG das Verarbeiten personenbezogener Daten nur auf Basis eines Erlaubnistatbestandes zulässig. Ein Ausgangspunkt ist das Verbot einer Verarbeitung.

B. Datenschutz bei den konkreten Maßnahmen

Das Recht auf informationelle Selbstbestimmung, das das Bundesverfassungsgericht im Volkszählungsurteil aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitet hat, schützt die Bürger gegen eine unbegrenzte Erhebung und Verwendung ihrer persönlichen Daten. Einschränkungen dieses Rechts bedürfen einer gesetzlichen Grundlage, die vor der verfassungsmäßigen Ordnung Bestand haben und insbesondere dem Grundsatz der Verhältnismäßigkeit genügen muss.[158] Eine Erhebung und Verwendung persönlicher Daten auf Grundlage der einfachgesetzlichen Ermächtigung stellt insoweit eine von der Verfassung gebotene Einschränkung des Grundrechts auf informationelle Selbstbestimmung dar und soll in der Prüfung der Verhältnismäßigkeit als sog. Schranken-Schranke bestehen. Wegen seiner erheblichen Bedeutung im Hinblick auf die starke Betroffenheit der privaten Lebensgestaltung wird aus dem Grundrecht ferner der Grundsatz der Zweckbindung personenbezogener Daten gefolgert. Die Forderung der strikten Zweckbindung ist angesichts der mit der heutigen

158 BVerfGE 65, 1 (41 ff.); BVerfGE 78, 77 (84 ff.); BVerfGE 80, 367 (373); BVerfGE 115 (320 ff.); BVerfGE 124, 78 (78 ff.); BVerfGE 125, 260 (260 ff.).

elektronischen Datenverarbeitung verbundenen Gefahren selbstverständlich.

Auf der Grundlage dieser Erkenntnisse soll im Folgenden untersucht werden, ob die Verwertung persönlicher Daten in den oben ausgewählten Bereichen – also dem Strafregister, der Rasterfahndung und der Vorratsdatenspeicherung – den verfassungsrechtlichen Anforderung genügt und ob dabei die verfassungsrechtlich gebotenen Schutzvorkehrungen gegen einen unbefugten oder übermäßigen Zugriff auf die Daten hinreichend vorbereitet sind.

I. Strafregister

Gerichte, Staatsanwaltschaften und andere Justizbehörden sind gemäß § 474 StPO und § 41 BZRG dazu berechtigt, personenbezogene Daten aus dem Strafregister für Zwecke der Rechtspflege zu verwenden. Für die Erhebung und Verwendung personenbezogener Daten aus dem Strafregister im Strafverfahren bieten also §§ 474 bis 495 StPO die gesetzliche Ermächtigungsgrundlage. Die Verwendungszwecke beschränken sich auf die dort genannten Zwecke. Während § 161 Abs. 1 Satz 1 und 2 sowie § 163 Abs. 1 Satz 2 die Erhebung von Auskünften innerhalb desselben Verfahrens regeln, normieren §§ 474 Abs. 1, 478 Abs. 1 Satz 5 die Weitergabe von bereits in anderen, vorangegangenen Verfahren ermittelten Erkenntnissen für Zwecke der Rechtspflege.[159]

Die Speicherung strafrechtlich relevanter Daten spielt im Strafverfahren eine große Rolle. Daher wurden schon seit langem die zahlreichen Strafregister der Staatsanwaltschaften bei den Landgerichten und das Bundesstrafregister zur Verfügung gestellt,[160] das seit 1954 durch den Generalbundesanwalt beim BGH geführt wurde. Im Jahr 1972 wurden beide mit dem Bundeszentralregister in ein einheitliches, zentrales Register der Justiz integriert, das noch immer durch den Generalbundesanwalt beim BGH – Dienststelle Bundeszentralregister – in Berlin geführt wird.[161] Außerdem kann, wenn von Strafregistrierung gesprochen wird, nicht über das Straf-

159 *Schmitt*, Strafprozessordnung, § 474, Rn. 2; *Gieg*, KK-StPO, § 474 Rn. 1.

160 Vgl. Allg. Verwaltungsvorschriften des BMJ vom 27. Januar und vom 6. Juli 1954 (BAnz Nr. 21 und 129).

161 Dies geschah durch das am 1. Januar 1972 in Kraft getretene Gesetz über das Zentralregister und das Erziehungsregister (Bundeszentralregistergesetz – BZRG) vom 18. März 1971.

verfahrensregister gemäß §§ 492 ff. StPO hinweggesehen werden. Die gesetzliche Grundlage für ein länderübergreifendes staatsanwaltschaftliches Verfahrensregister wurde durch das Verbrechensbekämpfungsgesetz vom 28. Oktober 1994[162] erstmals in die StPO eingefügt und durch das Strafverfahrensänderungsgesetz 1999 vom 11. August 2000[163] geändert und erweitert. Dem Strafverfahrensregister kommt auch deshalb eine Bedeutung zu, weil die möglichen Gefahren im Hinblick auf die Frage des Datenschutzes bei einer Strafregistrierung als nicht gering einzuschätzen sind.

Um Aussagen darüber treffen zu können, wie die persönlichen Daten beim Strafregister geschützt werden, wird zunächst analysiert, wie die Strafregistrierung organisiert ist, was wie lange und wozu erhoben und gespeichert wird und welche Vorkehrungen zum Datenschutz getroffen werden (was also passieren kann, wenn die personenbezogenen Daten auch nach Ablauf eines bestimmten Zeitraums nicht gelöscht werden). Deshalb soll im Folgenden zunächst ein Überblick über das Strafregistersystem gegeben und dann auf die genannten Fragen eingegangen werden. Damit können die gegen die mit der automatisierten Datenverarbeitung verbundenen Gefahren vorgesehenen Schutzmaßnahmen unter dem Aspekt Datenschutz analysiert werden.

1. Organisationsstruktur

Die personenbezogenen Daten, die im Strafverfahren verwertet werden dürfen, können hauptsächlich aus dem Bundeszentralregister (BZR) und dem zentralen staatsanwaltschaftlichen Verfahrensregister (ZStV) erhalten werden. Während es sich beim BZR grundsätzlich um gerichtliche Verurteilungen handelt, betrifft das ZStV das Ermittlungs- und Strafverfahren der Staatsanwaltschaft. Dieser Regelungsbereich gehört also zum unmittelbaren Vorfeld des gerichtlichen Verfahrens. Angesichts der Besonderheiten des Jugendstrafrechts und der darin normierten vorwiegend auf erzieherische Wirkungen abstellenden Maßnahmen ist in das BZR ein gesondertes Erziehungsregister (§§ 55 ff. BZRG) integriert, in dem derartige Entscheidungen gegen Jugendliche gesondert registriert werden.

---

162 Gesetz zur Änderung des Strafgesetzbuches, der Strafprozessordnung und anderer Gesetze (Verbrechensbekämpfungsgesetz) vom 28. Oktober 1994, BGBl. I 1994, S. 3186.

163 Gesetz zur Änderung und Ergänzung des Strafverfahrensrechts – Strafverfahrensänderungsgesetz 1999 (StVÄG 1999), BGBl. I 2000, S. 1253.

Im Folgenden soll die Organisationsstruktur dieser beiden Formen der Strafregistrierung untersucht werden. Dabei kann festgestellt werden, in welcher Form das Mitteilungs- und das Speicherungsverfahren von Daten im deutschen Strafregistersystem verlaufen.

a) Das Bundeszentralregister

Das BZR wurde mit gleichzeitiger Umstellung der Registerführung auf die elektronische Datenverarbeitung eingerichtet. Es setzte erhebliche organisatorische und technische Anstrengungen voraus, etwa die Übernahme der Altbestände und die zentrale Erfassung der aktuellen Entscheidungen bei gleichzeitiger Aufrechterhaltung des Auskunftsbetriebes.

Die Organisationsstruktur des BZR wird zuerst grob vorgestellt. Die mitteilungspflichtigen Stellen der Registerbehörde sollen die nach dem BZRG einzutragenden Entscheidungen übermitteln. Die Registerbehörde soll sie dann speichern und damit auf das Auskunftsersuchen antworten. Nach § 1 Abs. 1 BZRGVwV erfolgen die Mitteilungen an das Zentralregister durch die Vollstreckungsbehörde, die Verwaltungsbehörde, das Gericht und die Strafverfolgungsbehörde. Die mitteilungspflichtigen Stellen sollen die Formularmitteilungen mit speziellen Schreibmaschinen nach vorgegebenen Regeln ausfüllen und der Registerbehörde im Wege der Datenfernübertragung übermitteln. Die Mitteilungen sollen bei Entscheidungen binnen eines Monats nach Eintritt der Vollziehbarkeit, Unanfechtbarkeit oder Rechtskraft, bei rechtskräftigen strafgerichtlichen Verurteilungen (§ 3 Nr. 1 BZRG) binnen eines Monats nach Ablauf der gemäß § 275 Abs. 1 Satz 2 der Strafprozessordnung bestimmten Frist, bei Entscheidungen ohne solche Rechtswirkungen binnen eines Monats nach ihrem Erlass und bei anderen Tatsachen binnen eines Monats nach ihrem Eintritt übermittelt werden.[164] Die Formularmitteilungen werden dann beim BZR von einer Maschine eingelesen, die die maschinenschriftlichen Einträge optisch erkennt und in eine der Datenverarbeitungsanlage verständliche Sprache umsetzt. Die Mitteilungen werden, sobald sie vom Seitenleser-System gelesen und in einen Magnetbandsatz umgewandelt wurden, nach zahlreichen Plausibilitätsprüfungen programmgesteuert in das EDV-geführte Register eingegliedert. Bei der Einordnung von Neueintragungen wird eine Identitätsfeststellung durchgeführt.

164 § 3 BZRGVwV.

Auch die Anfragen (Ersuchen um Erteilung von Führungszeugnissen, unbeschränkte Auskünfte aus dem Zentralregister und Auskünfte aus dem Erziehungsregister von Gerichten und Behörden, Anträge von Privatpersonen auf Erteilung von Führungszeugnissen) sollen der Registerbehörde im Wege der Datenübertragung übermittelt werden (§ 4 I 1. Satz BZRGVwV). Die Beantwortung von Auskunftsersuchen, also die Auskunftserteilung aus dem BZR, erfolgt im Wege der Erteilung von Führungszeugnissen (§§ 30 bis 32 BZRG) und unbeschränkten Auskünften (§§ 41 und 42 BZRG). Um die personenbezogenen Daten im System zu schützen, erfordert das BZRG für die Einrichtung eines automatisierten Verfahrens, das die Übermittlung personenbezogener Daten durch Abruf ermöglicht, bestimmte Umstände, nämlich dass diese Übermittlungsform unter Berücksichtigung der schutzwürdigen Interessen der Betroffenen angemessen ist und dass gewährleistet ist, dass die Daten bei der Übermittlung wirksam gegen einen unbefugten Zugriff Dritter geschützt sind.[165] Bei der Datenfernübertragung sind dem jeweiligen Stand der Technik entsprechende Maßnahmen zur Sicherstellung von Datenschutz und -sicherheit zu treffen, die insbesondere die Vertraulichkeit und Unversehrtheit der Daten gewährleisten; im Falle der Nutzung allgemein zugänglicher Netze sind dem jeweiligen Stand der Technik entsprechende Verschlüsselungsverfahren anzuwenden. Die Registerbehörde lässt eine schriftliche Übermittlung durch Gerichte auf Vordrucken zu, soweit sie hierfür keine webbasierte Datenübertragungslösung bereitstellt. Im Übrigen kann die Registerbehörde eine schriftliche Übermittlung auf Vordrucken zulassen (§ 4 I Satz 2 bis 4 BZRGVwV).

Die beiden Auskunftserteilungsmöglichkeiten sind allerdings mit jeweils anderen Voraussetzungen und Einschränkungen verbunden. Beim Führungszeugnis ist je nach Verwendungszweck zwischen einem Privatführungszeugnis (§ 30 Abs. 1 BZRG) und einem Behördenführungszeugnis (§ 30 Abs. 5, § 31 BZRG) mit unterschiedlichen Inhalten zu differenzieren. Den inhaltlichen Unterschied gibt es ebenso bei der unbeschränkten Auskunft, ebenfalls je nach Empfängerkreis. In § 41 Abs. 3 BZRG ist vorgeschrieben, dass nur noch den Strafgerichten und den Staatsanwaltschaften für ein Strafverfahren gegen den Betroffenen Auskunft erteilt werden darf. Der Inhalt des Registers und die Verwertung der Auskünfte aus dem Register werden unten eingehender diskutiert.

165 § 21 Satz 1 BZRG.

b) Das länderübergreifende staatsanwaltschaftliche Strafverfahrensregister

Wie erwähnt, können die Daten, die im Strafverfahren verwertet werden dürfen, nicht nur aus dem BZR, sondern auch aus dem ZStV hergenommen werden. Letzteres kann allerdings nicht als das Strafregister im eigentlichen Sinne bezeichnet werden. Das in den §§ 492 bis 495 StPO geregelte länderübergreifende staatsanwaltschaftliche Verfahrensregister, dessen Einrichtung durch Art. 4 Nr. 1 des Gesetzes zur Änderung des Strafgesetzbuches, der Strafprozessordnung und anderer Gesetze – Verbrechensbekämpfungsgesetz – vom 28. Oktober 1994[166] in die Strafprozessordnung eingefügt wurde, wird vom Bundesamt für Justiz (BfJ)[167] als zentraler Dienstleistungsbehörde der Bundesjustiz mit Sitz in Bonn geführt.

Anders als das BZR soll das ZStV nach der Entwurfsbegründung dazu dienen, mit umfassenden und schnell verfügbaren Informationen über die bundesweit gegen einen Beschuldigten geführten Ermittlungs- und Strafverfahren der Staatsanwaltschaft die sachgerechte Führung eines Ermittlungsverfahrens zu erleichtern.[168] Damit will der Gesetzgeber insbesondere im Interesse der Allgemeinheit und der von den Strafverfolgungsmaßnahmen Betroffenen die Effektivität der Strafrechtspflege erhöhen.[169] Die Einrichtung des ZStV beruht also auf der Überlegung, dass zur Gewährleistung der Funktionstüchtigkeit der Strafrechtspflege auch die Verbesserung der Information der Staatsanwaltschaften gehört, damit Entscheidungen auf der Grundlage umfassender Erkenntnisse aus allen Ermittlungs- und Strafverfahren getroffen werden können. Dieser Regelungsbereich gehört zum unmittelbaren Vorfeld des gerichtlichen Verfahrens. Das heißt: Trifft ein Gericht eine im BZR einzutragende Entscheidung – sobald die Entscheidung also rechtskräftig geworden ist –, so erhält die Registerbehörde des BZR eine Mitteilung nach § 20 BZRG. Wird eine solche Entscheidung in das BZR eingetragen, so wird die entsprechende Eintragung im ZStV automatisch gelöscht.[170]

166 BGBl. I, S. 3186.

167 Das Register wurde seit Anfang 1999 bei der Dienststelle Bundeszentralregister des Generalbundesanwalts in Bonn geführt, seit dem 1. Januar 2007 beim Bundesamt für Justiz (BfJ), das aufgrund des Gesetzes zur Errichtung und zur Regelung der Aufgaben des Bundesamts für Justiz vom 17. Dezember 2006 neu eingerichtet wurde (BGBl. I, S. 3171–3174).

168 BT-Drs. 12/6853, S. 3.

169 BT-Drs. 12/6853, S. 37.

170 *Gieg*, KK-StPO, § 494 Rn. 4.

Das länderübergreifende staatsanwaltschaftliche Verfahrensregister ist als eine Datenbank zur Speicherung der anhängigen Ermittlungsverfahren konzipiert und wird sich in Teilen an die Struktur des BZR-Verfahrens anlehnen.[171] Zur Identifizierung eines Beschuldigten und zur sachgerechten Führung des Ermittlungsverfahrens teilt die mitteilungspflichtige Stelle, also die Staatsanwaltschaft oder die dieser in steuerstrafrechtlichen Angelegenheiten gleichgestellte Finanzbehörde, der Registerbehörde – Bundesamt für Justiz (BfJ) – insbesondere die Personendaten des Beschuldigten, die Tatzeiten und -vorwürfe, das Aktenzeichen sowie die Verfahrenseinleitung und -erledigung mit. Die Mitteilung erfolgt bei jedem Beschuldigten unabhängig von der Bedeutung der vorgeworfenen Tat. Über jeden Beschuldigten sind der Registerbehörde in jedem Fall zwei Mitteilungen zu machen: die Erstmitteilung über die Einleitung des Verfahrens sowie die Erledigungsmitteilung über den Abschluss des Ermittlungsverfahrens.[172] Mit diesen Informationen wird eine Vollspeicherung im Register erreicht. Die Einzelheiten legt die mit Zustimmung des Bundesrates erlassene Errichtungsanordnung des Bundesjustizministeriums gemäß § 494 Abs. 4 StPO fest.[173] Danach kann im Falle einer besonderen Geheimhaltungsbedürftigkeit des Strafverfahrens die Übermittlung unter Maßgabe der Norm erfolgen, dass Auskünfte über die übermittelten Daten an eine andere als die mitteilende Stelle ganz oder teilweise zu unterbleiben haben (§ 3 Abs. 2 ZStVBetrV). Daneben ist unter bestimmten Voraussetzungen auch die vorübergehende Zurückstellung der Übermittlung möglich (§ 3 Abs. 3 Satz 1 ZStVBetrV). Um dieses Register jederzeit aktuell zu halten, wird gefordert, dass die Übermittlung der vorhandenen Daten an die Registerbehörde grundsätzlich zeitgleich mit der Einleitung eines Ermittlungsverfahrens vorgenommen wird (§ 3 Abs. 1 Satz 1 ZStVBetrV).

Die Datenübermittlung erfolgt grundsätzlich im Wege eines automatisierten Abrufverfahrens oder eines automatisierten Anfrage- und Auskunftsverfahrens, also im Wege der Datenfernübertragung. Auf Ersuchen mit nicht eindeutig zuordenbaren oder unvollständigen Identifizierungsdatensätzen übermittelt die Registerbehörde an die ersuchende Stelle für Zwecke der Identitätsprüfung die in § 4 Abs. 1, 2 Satz 1 Nr. 1 und 2 sowie Abs. 3 bezeichneten Daten von bis zu zwanzig unter ähnlichen Identifizie-

171 BT-Drs. 13/386.

172 *Hilger*, LR-StPO, § 492 Rn. 20.

173 Verordnung über den Betrieb des Zentralen Staatsanwaltschaftlichen Verfahrens-registers (ZStVBetrV) vom 23. September 2005.

rungsdaten gespeicherten Personen und teilt mit, wie viele weitere Datensätze zu Personen mit ähnlichen Identifizierungsdaten vorhanden sind.

2. Inhalt des Registers

a) Das Bundeszentralregister

Durch das BZRG wurde die Registeraufgabe wesentlich erweitert. § 3 BZRG schreibt vor, welche Daten in das Register einzutragen sind. Danach sind neben rechtskräftigen strafgerichtlichen Verurteilungen (§§ 4 bis 9 BZRG), Entmündigungen (§ 10 Abs. 1 BZRG) und Vermerken über Schuldunfähigkeit (§ 12 Abs. 1 BZRG) auch bestimmte Entscheidungen von Verwaltungsbehörden und Gerichten (§ 11 BZRG) einzutragen. Außerdem werden die gerichtlichen Entscheidungen registriert, die im Zusammenhang mit Betäubungsmittelabhängigkeit stehen (§ 17 Abs. 2 BZRG), sowie diejenigen Entscheidungen, die eine im Zusammenhang mit der Ausübung eines Gewerbes begangene Tat betreffen (§§ 18, 32 Abs. 4 BZRG). Ferner können Suchvermerke und Steckbriefnachrichten im Register niedergelegt werden (§ 25 BZRG). Gemäß § 54 BZRG müssen ebenso strafgerichtliche Verurteilungen ausländischer Gerichte in das BZR eingetragen werden, wenn sie sich auf deutsche Staatsbürger oder im Geltungsbereich des BZR geborene oder wohnhafte Ausländer beziehen und eine Straftat betreffen, die nach deutschem Recht ein Vergehen oder Verbrechen darstellt. Wenn strafrechtliche Verurteilungen Deutscher durch einen anderen Mitgliedstaat der Europäischen Union deshalb nicht in das Register einzutragen sind, weil die Voraussetzungen des § 54 Abs. 1 Nr. 2 BZRG nicht erfüllt sind, müssen diese durch das BfJ im Register gesondert gespeichert werden (§ 56b BZRG). Die Speicherungen dürfen an einen anderen Mitgliedstaat nur zur Unterstützung eines strafrechtlichen Verfahrens in diesem Staat auf Grund eines Ersuchens übermittelt werden.

Entscheidungen und Anordnungen, die in Anbetracht der Besonderheiten des Jugendstrafrechts, das vorwiegend auf den Erziehungsgedanken abzielt, in das Erziehungsregister eingetragen werden, sind gesondert in § 60 BZRG geregelt. Gespeichert werden Anordnungen von Maßnahmen nach § 3 Satz 2 JGG sowie Erziehungsmaßregeln oder Zuchtmittel, Schuldsprüche, Anordnungen des Familiengerichts sowie Freisprüche oder Verfahrenseinstellungen wegen mangelnder Reife.

Im Hinblick auf die erweiterte Aufgabe des Registers ist der Begriff "Strafregister" durch den nicht als diskriminierend empfundenen neutralen Begriff "Bundeszentralregister" ersetzt worden.[174]

b) Das länderübergreifende staatsanwaltschaftliche Strafverfahrensregister

Die in das ZStV einzutragenden Daten regeln § 492 Abs. 2 StPO und § 4 ZStVBetrV. In den Vorschriften werden die einzutragenden Daten abschließend ausgeführt. Es dürfen danach keine anderen Daten als die Personendaten der beschuldigten Person, die Daten zur Straftat, Vorgangsdaten wie etwa die mitteilende Stelle, die sachbearbeitende Stelle der Polizei sowie die Aktenzeichen und die Daten zum Verfahrensstand gespeichert werden. Im ZStV werden also die Daten neu eingeleiteter, laufender und auch bereits eingestellter Ermittlungsverfahren über alle beschuldigten Personen unabhängig vom Gewicht vorgeworfener Taten gespeichert.

3. Verwendung der Daten aus dem Register

a) Das Bundeszentralregister

Das Strafregister stellt sich durch die einheitliche Einrichtung von Strafverzeichnissen auf die umfassende Versorgung – insbesondere der Justizbehörden – mit den erforderlichen Informationen ein. Damit wird der Zugang zu zuverlässigen Angaben über die kriminelle Vergangenheit sowie zu anderen für die Beurteilung der Persönlichkeit eines Beschuldigten wichtigen Gesichtspunkten als Voraussetzung für Täterschaftsindiz, Strafzumessung und Rückfallverschärfung gewährleistet.[175] Hierbei sind die Regelungen des Bundeszentralgesetzes bedeutsam. Da bei der Verwendung von Daten aus dem Register stets die Gefahr besteht, dass hochsensible Daten wie etwa eine Verurteilung oder eine sonst eintragungspflichtige Tatsache gegen den Willen des Bestraften bekannt werden und diesem dadurch Nachteile entstehen, wird bei der Verwendung der Daten aus dem Register besondere Sorgfalt gefordert. Daraus folgen verfassungsrechtliche Anforderungen wie Zweckbindungsgrundsatz, Datensparsamkeit usw.

174 *Tolzmann*, Bundeszentralregistergesetz, S. 9.
175 *Rebmann*, Einhundert Jahre Strafregisterwesen in Deutschland, NJW 1983, 1513, 1513.

Die Registereintragungen werden grundsätzlich im Wege des Privat- sowie Behördenführungszeugnisses und der unbeschränkten Auskunft angekündigt. Auch Eintragungen ausländischer Verurteilungen im Zentralregister sind entsprechend den für deutsche Verurteilungen geltenden Regelungen in Führungszeugnisse und Auskünfte aus dem Register aufzunehmen. Über Führungszeugnisse wird Auskunft über die eine bestimmte Person betreffenden Inhalte des BZR grundsätzlich auf Antrag des Betroffenen (§ 30 BZRG) und ausnahmsweise auf Anforderung von Behörden (§ 31 BZRG) erteilt. Die Daten, die im Strafverfahren verwendet werden dürfen, erhalten bestimmte Behörden, z. B. Gerichte und Staatsanwaltschaften, für die in § 41 BZRG genannten Zwecke (z. B. in Strafverfahren, vor der Erteilung eines Waffenscheines, vor einer Einbürgerung, vor einer Verbeamtung usw.). Sie können diesbezüglich eine unbeschränkte Auskunft in Anspruch nehmen und einen entsprechenden Auszug aus eigener Veranlassung direkt beim Bundesamt für Justiz anfordern, ohne dass der Betroffene davon Kenntnis erhält. In unbeschränkten Auskünften sind auch solche Eintragungen enthalten, die nicht oder jedenfalls nicht mehr in das Führungszeugnis aufzunehmen sind.

aa) Führungszeugnis

Im Privatführungszeugnis, das auf Antrag jeder Person, die das 14. Lebensjahr vollendet hat, oder ihres gesetzlichen Vertreters erteilt wird, wird nur ein begrenzter Ausschnitt der tatsächlich möglichen Eintragungen aufgenommen. Die in das Führungszeugnis aufzunehmenden und nicht aufzunehmenden Inhalte regelt im Einzelnen § 32 BZRG. Das Führungszeugnis kann für eigene Zwecke (Privatführungszeugnis) oder zur Vorlage bei einer deutschen Behörde (Behördenführungszeugnis) erteilt werden. Der Inhalt des Behördenführungszeugnisses geht dabei über das Privatführungszeugnis hinaus (§ 32 Abs. 3, 4 BZRG). Weiters hat jede Person, die das 14. Lebensjahr vollendet hat, gemäß § 42 BZRG einen Anspruch auf eine Auskunft darüber, welche Eintragungen über sie im Register enthalten sind. Die Mitteilung kann durch Einsichtnahme bei der Registerbehörde oder durch Übersendung der Auskunft an ein von der betroffenen Person benanntes Amtsgericht erfolgen, bei dem die betroffene Person die Auskunft persönlich einsehen kann. Ein Antrag nach § 42 BZRG ist schriftlich oder durch persönliches Erscheinen an das BfJ (Referat IV 1) zu richten. Dieser muss die vollständigen Personendaten der antragstellenden Person (Geburtsname, Familienname, sämtliche Vornamen, Geburts-

datum und -ort) enthalten. Ein Privatführungszeugnis ist im Hinblick auf den Aspekt der Wiedereingliederung der Bestraften in Beruf und Gesellschaft oder des Datenschutzes jedoch nicht unproblematisch. Zum Beispiel werden Führungszeugnisse als datenschutzrechtliche Selbstauskunft in großem Umfang von der Arbeitgeberseite gefordert und damit von den Stellenbewerberinnen und -bewerbern beantragt. Zweifelhaft erscheint, ob das privatwirtschaftliche Interesse an der Gewinnung unbestrafter Mitarbeiterinnen und Mitarbeiter als schutzbedürftiges Allgemeininteresse gelten kann.[176]

Behörden erhalten grundsätzlich in Form eines Führungszeugnisses Auskunft aus dem Register, das in der Regel von der betroffenen Person beantragt wird. Behörden können gemäß § 31 BZRG jedoch auch selbst ein Führungszeugnis beantragen, soweit sie es zur Erledigung ihrer hoheitlichen Aufgaben benötigen und eine Aufforderung an die betroffene Person, ein Führungszeugnis vorzulegen, nicht sachgemäß ist oder erfolglos bleibt (§ 31 Abs. 1 S. 2 BZRG). Die Behörde hat der betroffenen Person auf Antrag Einsicht in ihr Führungszeugnis zu gewähren. Nach § 31 BZRG wird ausnahmslos sämtlichen Behörden die Möglichkeit gegeben, für alle ihnen geeignet erscheinenden Zwecke über jedermann ein Führungszeugnis anfordern zu können, sofern nur eine hoheitliche Aufgabe zu erledigen ist. Die Vorschrift scheint aber schwer mit den verfassungsrechtlichen Anforderungen zum Datenschutz vereinbar, da der Verwendungszweck weder bereichsspezifisch noch präzise bestimmt ist. Vielmehr kann das Behördenführungszeugnis auf der Grundlage einer Generalklausel angefordert werden, ohne dass gesichert wäre, dass die spezifisch hoheitlichen Zwecke, für die das Führungszeugnis angefordert wird, die Offenlegung der im Führungszeugnis enthaltenen Angaben gerade für diesen Zweck erfordern. Noch bedenklicher ist, dass die Behörde die Bereitschaft der Betroffenen, ein ihnen auf Antrag erteiltes Führungszeugnis selbst beizubringen, unter der oben genannten, kaum objektivierbaren Voraussetzung übergehen kann und dass die Anforderung an die Betroffenen, ein Führungszeugnis vorzulegen, nicht sachgemäß ist, womit dann auch die Möglichkeit der Betroffenen ausgehebelt wird, auf Verlangen Einsicht in das Führungszeugnis zu nehmen. Hier müsste zumindest eine Pflicht der Behörden festgeschrieben werden, zum nachträglichen Rechtsschutz des Betroffenen den Grund ausdrücklich zu dokumentieren, aus dem sie eingeschätzt haben, dass die Vorlegung eines Führungszeugnisses durch den

176 *Tolzmann*, Bundeszentralregistergesetz, S. 12.

Betroffenen nicht zu erwarten ist, und dass die Betroffenen nachträglich von der Einholung des Führungszeugnisses in Kenntnis zu setzen sind.[177]

Die in das Führungszeugnis aufgenommenen Eintragungen bestehen nicht dauerhaft. Die Nichtaufnahme von Verurteilungen in das Führungszeugnis unterscheidet sich von der Tilgung als der endgültigen und unwiederbringlichen Entfernung von Eintragungen im Zentralregister darin, dass Eintragungen bloß im Führungszeugnis nicht mehr angezeigt werden, im Register aber noch verbleiben. Die Aufnahme in das Führungszeugnis hängt von einer Frist ab, die sich grundsätzlich nach der Höhe der Strafe richtet, unabhängig von dem der Verurteilung zugrunde liegenden Delikt. Die Nichtaufnahmefrist beträgt meist fünf Jahre (§ 34 Abs. 1 BZRG), nur ausnahmsweise drei Jahre bei § 34 Abs. 1 Nr. 1 BZRG und zehn Jahre bei § 34 Abs. 1 Nr. 2 BZRG. Sind im Register mehrere Verurteilungen eingetragen, so sind, solange eine von ihnen in das Zeugnis aufzunehmen ist, alle in das Führungszeugnis aufzunehmen (Mitzieheffekt, § 38 Abs. 1 BZRG). Die Regelung kennt Ausnahmen in § 38 Abs. 2 BZRG.

Die Nichtaufnahme von Verurteilungen in das Führungszeugnis kann mit einer Anordnung der Registerbehörde auf Antrag oder von Amts wegen geschehen, soweit diese Anordnung nicht dem öffentlichen Interesse entgegensteht. Die Fristverkürzungsmöglichkeit dient dazu, besonderen Umständen, die in Tat oder Täterpersönlichkeit begründet sein mögen, durch eine Einzelfallentscheidung Rechnung zu tragen.[178] Die Möglichkeit beschränkt sich auf eng begrenzte Ausnahmefälle. Dadurch wird der Interessenwiderstreit zwischen dem öffentlichen Interesse an der Vollständigkeit des Registers und dem Rehabilitationsinteresse des Betroffenen bereits durch die nach der Höhe der Verurteilungen gestaffelten Fristen berücksichtigt.[179]

bb) Unbeschränkte Auskunft

Unter dem Aspekt des Schutzes persönlicher Daten im Strafverfahren hat die unbeschränkte Auskunft eine erhebliche Bedeutung. Bestimmten, in

177 *Tolzmann*, Bundeszentralregistergesetz, S. 15.

178 *Siebrasse*, Strafregistrierung und Grundgesetz – Zur Verfassungsmäßigkeit der Straf(verfahrens)registrierung in BZRG, StPO, BKAG und BGSG, S. 10.

179 Dazu ausführlich *Siebrasse*, Strafregistrierung und Grundgesetz – Zur Verfassungsmäßigkeit der Straf(verfahrens)registrierung in BZRG, StPO, BKAG und BGSG, S. 11 ff.; *Kalf*, Die Fristen des Bundeszentralregistergesetzes in der strafrechtlichen Praxis, StV 1991, 137, 138 f.

§ 41 BZRG aufgeführten Stellen (u. a. Gerichten, Staatsanwaltschaften sowie bestimmten Behörden) ist durch die Registerbehörde auf Antrag eine unbeschränkte Auskunft aus dem Zentralregister zu erteilen. In Auskünfte an diese Stellen sind auch solche Eintragungen aufzunehmen, die nicht oder nicht mehr in Führungszeugnisse aufzunehmen sind. In diese Auskünfte wird also der gesamte Inhalt des Registers aufgenommen, auch nach Ablauf bestimmter Nichtaufnahmefristen. Hierbei gibt der Gesetzgeber dem Interesse der Allgemeinheit an der Abwehr besonderer Gefahren Vorrang vor dem Interesse des Betroffenen an einer möglichst reibungslosen Wiedereingliederung.[180]

Bei einer Auskunftsanfrage fordert das BZRG zum Schutz vor einem übermäßigen Zugriff die Zweckbindung, damit bei einer Anfrage eine Zweckangabe gesetzlich vorgesehen ist, die von der Registerbehörde darauf geprüft wird, ob der angegebene Zweck ein Recht auf unbeschränkte Auskunft begründet. Für den Schutz dieser hochsensiblen Daten sind die auskunftsberechtigten Stellen in Verbindung mit der Beschränkung der Auskunftserteilung auf bestimmte Zwecke eng begrenzt und abschließend aufgezählt. Darin werden die Gerichte, Gerichtsvorstände, Staatsanwaltschaften und Aufsichtsstellen (§ 68a des StGB) für Zwecke der Rechtspflege sowie die Justizvollzugsbehörden für Zwecke des Strafvollzugs einschließlich der Überprüfung aller im Strafvollzug tätigen Personen ernannt. Dies gilt also auch für die Nutzung der Daten im Strafverfahren für die Strafrechtspflege. Die unbeschränkte Auskunft wird nur auf ausdrückliches Ersuchen erteilt (§ 41 Abs. 4 BZRG). In diesem Ersuchen muss angegeben werden, aus welchem Grund die angeforderte Auskunft erforderlich ist, die dann ausschließlich zu dem genannten Zweck verwendet werden darf. Grundsätzlich ist das Ersuchen auf einem Vordruck mit einer Zweckangabe an die Registerbehörde zu richten; heute ergeht es aber weitgehend auf elektronischem Weg.[181] Die Weitergabe von Eintragungen, die nicht in ein Führungszeugnis aufgenommen werden, ist nur dann erlaubt, wenn dies zur Vermeidung von Nachteilen für den Bund oder ein Land unerlässlich ist oder wenn andernfalls die Erfüllung öffentlicher Aufgaben erheblich gefährdet oder erschwert würde (§ 43 BZRG). Die Weitergabe von Führungszeugnissen für Behörden an eine andere Behörde ist erlaubt,

180 Vgl. OLG Hamm, NStZ 1985, 558 (558); *Tolzmann*, Bundeszentralregistergesetz, § 39 Rn. 4, 17, § 30 Rn. 6 ff.; *Rebmann/Uhlig*, BZRG, § 39, Rn. 31 ff.; *Siebrasse*, Strafregistrierung und Grundgesetz – Zur Verfassungsmäßigkeit der Straf(verfahrens)registrierung in BZRG, StPO, BKAG und BGSG, S. 10.

181 *Tolzmann*, Bundeszentralregistergesetz, § 41 Rn. 65 f.

wenn bei dieser die Voraussetzung, nämlich die Einwilligung der Betroffenen, erfüllt ist. Schranken wie etwa die abschließende Aufzählung der auskunftsberechtigten Stellen, die grundsätzliche Begrenzung auf Einzelanfragen oder die Beschränkung der Auskunftserteilung auf bestimmte Zwecke sind also gesetzlich eingebaut worden, um den Schutz personenbezogener Daten zu gewährleisten und damit unberechtigten oder übermäßigen Zugriff auf diese Daten zu vermeiden. Die Auskünfte aus dem Zentralregister an Behörden (§ 30 Abs. 5, §§ 31, 41, 43 BZRG) beschränken sich außerdem auf den mit der Entgegennahme oder Bearbeitung betrauten Bediensteten (§ 44 BZRG), damit das Interesse der Betroffenen an einer weitestgehenden Geheimhaltung ihrer Daten garantiert werden kann.

Da die vorliegende Arbeit darauf abzielt, die Frage des Schutzes personenbezogener Daten im Strafverfahren oder, genauer gesagt, die des Schutzes der für Strafverfahren verwendeten personenbezogenen Daten im Strafverfahren, zu untersuchen, aber nicht die des Schutzes der personenbezogenen Daten in sämtlichen Bereichen, wird die Frage des Führungszeugnisses hier nicht weiter diskutiert. Im Mittelpunkt steht vielmehr die unbeschränkte Auskunft, die den Justizbehörden im Strafverfahren erteilt wird.

b) Das länderübergreifende staatsanwaltschaftliche Strafverfahrensregister

Die im ZStV erhobenen Daten dürfen grundsätzlich nur für Strafverfahren gespeichert, verändert und verwendet werden (§ 492 Abs. 2 S. 2, Abs. 6 StPO) und grundsätzlich erhalten nur die Strafverfolgungsbehörden Auskünfte aus dem ZStV, und zwar ausschließlich zum Zweck der Verwendung im Strafverfahren. Dabei spielt es keine Rolle, ob die Verwertung in dem Verfahren erfolgt, in dem übermittelt wurde, oder in einem anderen. Zu den Strafverfolgungsbehörden gehören hierbei neben den Staatsanwaltschaften und den Finanzbehörden in Ermittlungsverfahren nach §§ 399, 386 AO auch die Polizeibehörden, die Finanzbehörden in Ermittlungsverfahren nach § 402 AO sowie die Steuer- und Zollfahndungsdienststellen, soweit sie im Einzelfall strafverfolgend tätig sind. Nach dem Zweckbindungsgrundsatz ist also die Verwertung personenbezogener Daten aus dem ZStV nur auf ihre Verwendung im Strafverfahren eingeschränkt. Um unnötigen Aufwand zu vermeiden, dürfen allerdings auch den Verfassungsschutzbehörden des Bundes und der Länder, dem Amt für den Militärischen Abschirmdienst und dem Bundesnachrichtendienst Auskünfte erteilt werden, sofern diesen ein Auskunftsrecht gegenüber den

Strafverfolgungsbehörden zusteht. In diesem Fall beschränken sich die Auskünfte auf die in § 492 Abs. 2 Satz 1 Nr. 1 und 2 StPO genannten Daten. Für den Erhalt weiterer Auskünfte wenden sich die Dienste unmittelbar an die betreffenden Staatsanwaltschaften. Um einen unbefugten oder übermäßigen Eingriff in das Recht der Bürger auf informationelle Selbstbestimmung abzuwehren, sind beim ZStV verschiedene Maßnahmen sichergestellt. So ist die Anzahl der Datensätze, die auf Grund eines Abrufs übermittelt werden dürfen, auf das für eine Identifizierung notwendige Maß zu begrenzen (§ 492 Abs. 4a Satz 4 und Abs. 6 StPO). Angesichts der mit der automatisierten Datenverarbeitung verbundenen Gefahr und der besonderen Schutzbedürftigkeit der im Register gespeicherten Daten wird ferner gefordert, dass die erforderlichen und angemessenen Maßnahmen getroffen werden, um die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der im Register gespeicherten Daten entsprechend dem jeweiligen Stand der Technik sicherzustellen. Für die Zulässigkeit des einzelnen automatisierten Abrufs ist grundsätzlich der Empfänger verantwortlich. Die Registerbehörde muss allerdings nach § 493 Abs. 3 Satz 3 ein Stichprobenverfahren durchführen.[182] Nach § 10 Abs. 2 BDSG ist es gewährleistet, dass die Zulässigkeit des Abrufverfahrens kontrolliert werden kann.

4. Speicherdauer

a) Das Bundeszentralregister

Eintragungen, die nach dem BZRG gespeichert werden, bleiben nicht ewig im BZR gespeichert, sondern werden unter bestimmten Voraussetzungen getilgt, es sei denn, es handelt sich um eine Verurteilung zu lebenslanger Freiheitsstrafe oder aber die Unterbringung in der Sicherungsverwahrung oder in einem psychiatrischen Krankenhaus wurde angeordnet (§ 45 BZRG).

Die Tilgung besteht in der vollständigen Entfernung der Eintragung aus dem Register durch die Löschung des Datensatzes auf dem Datenträger. Das bedeutet, dass nach der Entfernung niemand mehr – auch nicht die Registerbehörde selbst – Zugriff auf diese Daten nehmen und damit Kenntnis von ihnen erlangen kann. Neben der Nichtaufnahme bestimmter Eintragungen in das Führungszeugnis unterliegen die Regis-

182 Kritisch zur Praktikabilität *Gemählich*, KMR, § 493 Rn. 5; *Hilger*, LR-StPO, § 493 Rn. 20.

tereintragungen der fristgebundenen (§§ 45 bis 47) oder der fristunabhängigen Tilgung (§§ 48, 49). § 16 Abs. 2 BZRG regelt die fristunabhängige Entfernung von Entscheidungen aus dem Register, wenn sie in einem Wiederaufnahmeverfahren rechtskräftig aufgehoben wurden. In § 24 BZRG ist außerdem die Möglichkeit geregelt, die Eintragungen drei Jahre nach dem Eingang der Mitteilung oder der Vollendung des 90. Lebensjahres der von diesen Eintragungen betroffenen Person oder nach dem Todeseintritt zu entfernen, wenn ihr Tod gegenüber der Registerbehörde glaubhaft gemacht wurde.[183] Die Vorschrift zielt darauf ab, einem stetigen Anwachsen des Registers durch Belassen überholter Eintragungen entgegenzuwirken.[184] Außerdem werden Eintragungen im Erziehungsregister entfernt, sobald der Betroffene das 24. Lebensjahr vollendet hat (§ 63 Abs. 1 BZRG).

In besonderen Fällen können Eintragungen aufgrund einer Anordnung auch unabhängig von der Tilgungsfrist getilgt werden, falls die Vollstreckung erledigt ist und das öffentliche Interesse der Anordnung nicht entgegensteht (§ 49 BZRG). Damit kann das Bedürfnis befriedigt werden, die gesetzlich festgelegten Tilgungsfristen aus Gründen der Einzelfallgerechtigkeit um der Rehabilitation und der Resozialisierung des Betroffenen willen abzukürzen. Die Anordnung kann auf Antrag oder von Amts wegen erfolgen, sofern die Registerbehörde aus anderem Anlass einen Registerstand erkennt, der den Betroffenen unverhältnismäßig belastet. Die vorzeitige Tilgung aufgrund einer Anordnung setzt ähnlich wie bei der vorzeitigen Nichtaufnahme einer Verurteilung in das Führungszeugnis voraus, dass die Vollstreckung erledigt ist und das öffentliche Interesse der Anordnung nicht entgegensteht. Sie ist aber nur in außergewöhnlichen Härtefällen möglich, bei denen die Versagung der Registervergünstigung in der Bevölkerung auf Unverständnis stoßen würde.[185] Wenn die Registerbehörde den Antrag für unzulässig oder unbegründet erklärt, kann der Betroffene die Beschwerde führen.

Die Tilgung aufgrund eines Fristablaufs als ein Regelfall erfolgt automatisch, also ohne weitere Überprüfung und ohne besonderen Antrag

183 Die Entfernung einer Eintragung unterscheidet sich von der Tilgung: Mit der Entfernung sind keine materiellen Rechtswirkungen verbunden. Das heißt, weder das Verwertungsverbot nach § 51 noch das Schweigerecht nach § 53 I Nr. 2 gilt für entfernte Eintragungen. Außerdem werden auch Eintragungen entfernt, für die die Tilgung nicht in Betracht kommt (*Tolzmann*, Bundeszentralregistergesetz, § 24 Rn. 9 ff.).

184 *Tolzmann*, Bundeszentralregistergesetz, § 24 Rn. 4.

185 *Sawade/Schomburg*, Ausgewählte Probleme des Bundeszentralregistergesetzes, NJW 82, 551, 555.

seitens der Betroffenen. Bereits bei der Einordnung von Entscheidungen in das Register werden die Fristen für die Aufnahme in Führungszeugnisse sowie für die unbeschränkten Auskünfte und für die Tilgung von einem Fristenprogramm berechnet. Wird bei der täglichen Überprüfung der Tilgungsfristen festgestellt, dass Eintragungen gelöscht werden müssen, wird die Nummer des Satzes in eine Löschtabelle eingetragen. Der Satz wird anschließend von einem besonderen Löschprogramm untersucht, das sodann die Löschung vornimmt.[186] Bei der fristgebundenen Tilgung richtet sich die Länge der Tilgungsfrist gemäß §§ 46 ff. BZRG im Grundsatz nach der Höhe der Hauptstrafe.[187] Das BZRG regelt jede konkrete Tilgungsfrist nach den verhängten Strafen. Die Tilgungsfrist beträgt fünf Jahre bei Verurteilungen zu einer Geldstrafe von nicht mehr als neunzig Tagessätzen oder zu einer Freiheitsstrafe oder Strafarrest von nicht mehr als drei Monaten, zehn Jahre bei Verurteilungen zu einer Freiheitsstrafe oder Strafarrest von mehr als drei Monaten, aber nicht mehr als einem Jahr, zwanzig Jahre bei Verurteilungen wegen einer Sexualstraftat nach den §§ 174 bis 180 oder 182 StGB zu einer Freiheitsstrafe oder Jugendstrafe von mehr als einem Jahr oder fünfzehn Jahre in allen übrigen Fällen.

Der Ablauf der Tilgungsfrist einer Verurteilung wird durch weitere Verurteilungen gehemmt. Dies führt dazu, dass grundsätzlich alle Verurteilungen erst nach Ablauf der längsten Frist, die sich nicht zwingend nach der letzten Verurteilung bestimmt, gleichzeitig getilgt werden (§ 47 BZRG). Ergibt sich aus dem Register, dass die Vollstreckung einer Strafe oder eine der in § 61 des Strafgesetzbuches aufgeführten Maßregeln der Besserung und Sicherung noch nicht erledigt oder die Strafe noch nicht erlassen ist, ist der Ablauf der Tilgungsfrist ebenfalls gehemmt.

Der Tilgung werden die Rechtswirkungen, das Verwertungsverbot (§ 51 BZRG) und das Schweigerecht der Betroffenen (§ 53 I Nr. 2 BZRG) beigelegt. Von großer Bedeutung ist, dass die getilgte Eintragung in einem später gegen den Betroffenen anhängig gemachten Strafverfahren nicht mehr berücksichtigt werden darf. Ist die Eintragung über eine Verurteilung im Register getilgt worden oder ist sie zu tilgen, dürfen die Tat und die Verurteilung der betroffenen Person also im Rechtsverkehr nicht mehr

186 *Rebmann*, Einhundert Jahre Strafregisterwesen in Deutschland, NJW 1983, 1513, 1516 f.

187 Die tatsächliche Entfernung einer Eintragung erfolgt erst ein Jahr nach Ablauf der Tilgungsfrist im Register endgültig und unwiederbringlich (§ 45 Abs. 2 BZRG). Innerhalb eines Jahres werden bloß keine Auskünfte mehr erteilt. Die Tilgungsfrist betrifft also unmittelbar die Dauer des Anspruchs bestimmter Behörden auf unbeschränkte Auskunft aus dem Register.

vorgehalten oder zu ihrem Nachteil verwertet werden. Dabei umfasst das Verwertungsverbot nach der Rechtsprechung nicht bloß die Tatsache der Vorverurteilung als solche, sondern es untersagt auch die Berücksichtigung der Warnfunktion einer früheren Verurteilung zulasten des Angeklagten.[188] Ausnahmen von diesem Verwertungsverbot regelt § 52 BZRG. Aus der Tat oder der Verurteilung entstandene Rechte Dritter, gesetzliche Rechtsfolgen der Tat oder der Verurteilung und Entscheidungen von Gerichten oder Verwaltungsbehörden, die im Zusammenhang mit der Tat oder der Verurteilung ergangen sind, bleiben von der Tilgung unberührt.

Bei im Register eingetragenen ausländischen Entscheidungen ist deren rechtliche und inhaltliche Überprüfung durch das BfJ gesetzlich nicht vorgesehen. Eine Überprüfung ausländischer Entscheidungen kann nur in dem Staat erreicht werden, in dem die Entscheidung getroffen wurde, durch Einlegung des nach dem Recht dieses Staates zulässigen Rechtsbehelfs. Sofern dem BfJ die Aufhebung einer ausländischen Entscheidung durch den Entscheidungsstaat mitgeteilt wird, wird diese aus dem Register entfernt.

Das BZRG fordert in § 42 Satz 6 überdies, dass nach einer Einsichtnahme in Eintragungen über den Betroffenen im Register die Mitteilung von der Einsichtsstelle vernichtet wird.

b) Das länderübergreifende staatsanwaltschaftliche Strafverfahrensregister

Die Speicherdauer der in dem Strafverfahrensregister gespeicherten Daten ist in § 494 StPO festgeschrieben. Ihre Entfernung aus dem Register ist mit vier Voraussetzungen verbunden. Der erste Fall betrifft eine versehentliche Eintragung der Daten. Versehentlich eingetragene Daten müssen wieder entfernt werden, weil das ZStV nur solche Daten enthalten darf, deren Speicherung auch zulässig ist. Im zweiten Fall ist sichergestellt, dass Doppelspeicherungen im BZR und im länderübergreifenden ZStV vermieden werden. Wird also eine gerichtliche Entscheidung in das BZR eingetragen, so wird die entsprechende Eintragung im ZStV automatisch gelöscht. Drittens erfolgt die Löschung bei einem rechtskräftigen Freispruch, einer unanfechtbaren Ablehnung der Eröffnung des Hauptverfahrens und bei einer nicht nur vorläufigen, sondern endgültigen Verfahrenseinstellung,

188 BGHSt 24, 64 (65); BGHSt 28, 338 (340).

allerdings erst zwei Jahre nach der Verfahrenserledigung.[189] Schließlich erfolgt die Löschung in jenen Fällen, in denen dem ZStV ein weiteres Verfahren zu den vorher eingetragenen Daten mitgeteilt wurde, erst dann, wenn für alle Eintragungen die Löschungsvoraussetzungen vorliegen. Der Gesetzgeber hat außerdem in § 492 Abs. 4a Satz 2 und 3 StPO und § 8 Abs. 2 ZStVBetrV der ersuchenden Stelle die Pflicht auferlegt, nach erfolgter Identifizierung oder bei einer unmöglichen Identifizierung alle übermittelten Daten, die sich nicht auf den Betroffenen beziehen, unverzüglich zu löschen hat.

Die im ZStV gespeicherten Daten sind nach § 494 Abs. 3 i. V. m. § 489 Abs. 7 und 8 StPO zu sperren[190] statt zu löschen. Die Sperrung erfolgt, soweit potenziell günstige Informationen für den Betroffenen weiter verfügbar gehalten sowie Daten für laufende Forschungsarbeiten erhalten werden sollen, eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist oder wenn personenbezogene Daten nur zu Zwecken der Datensicherung oder der Datenschutzkontrolle gespeichert sind. Die gesperrten Daten dürfen verwendet werden, aber nur für den Zweck, für den die Löschung unterblieben ist, und auch nur, soweit dies zur Behebung einer bestehenden Beweisnot unerlässlich ist.

189 Nach der Entwurfsbegründung trägt die zweijährige Aufrechterhaltung der Speicherung trotz rechtskräftigen Freispruchs, unanfechtbarer Ablehnung der Eröffnung des Hauptverfahrens oder nicht nur vorläufiger Verfahrenseinstellung dem unverzichtbaren Informationsbedürfnis der Staatsanwaltschaften Rechnung (BT-Drs. 12/6853, S. 39). Diesbezüglich wird allerdings bezweifelt, ob dieses Informationsbedürfnis die für den Betroffenen eintretende Unschuldsvermutung in jedem Fall überwiegt (*Wolter*, Datenschutz und Strafprozeß, ZStW 1995, 793, 802; *Schmitt*, Strafprozessordnung, § 494, Rn. 9; *Temming/Schmidt*, HK-StPO, § 494 Rn. 10; *Kestel*, § 474 ff. StPO – eine unbekannte Größe, StV 1997, 266, 268; *Hellmann*, AK-StPO, § 476 Rn. 7). Der Entwurfsbegründung zustimmende Auffassung: *Kalf*, Die Fristen des Bundeszentralregistergesetzes in der strafrechtlichen Praxis, StV 1991, 137, 613; *Gieg*, KK-StPO, § 494 Rn. 6 unter Hinweis auf BVerfGE 74, 358; 82, 106.

190 Unter Sperrung ist die Kennzeichnung gespeicherter personenbezogener Daten zu verstehen, damit ihre weitere Verarbeitung oder Nutzung eingeschränkt werden kann (*Gieg*, KK-StPO, § 489 Rn. 6; *Schmitt*, Strafprozessordnung, § 489, Rn. 6; *Lemke*, NStZ 1995, 486).

II. Rasterfahndung

Die elektronische Datenverarbeitung durch die Strafverfolgungsbehörden begann bereits Ende der sechziger Jahre, aber ohne eine formalgesetzliche Grundlage.[191] Das Volkszählungsurteil des Bundesverfassungsgerichts, in dem anerkannt wird, dass die elektronische Datenverarbeitung personenbezogener Daten einen Eingriff in das aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG hergeleitete Recht auf informationelle Selbstbestimmung darstellen kann, machte die Schaffung präziser bereichsspezifischer gesetzlicher Grundlagen für die elektronische Datenverarbeitung erforderlich. In diesem Zusammenhang wurde die Rasterfahndung durch das Gesetz zur Bekämpfung des illegalen Rauschgifthandels und anderer Erscheinungsformen der Organisierten Kriminalität (OrgKG) vom 15. Juli 1992 in die StPO eingegliedert (§§ 98a – 98c). Da demnach jede Datenverarbeitung ohne einen gesetzlichen Erlaubnistatbestand grundsätzlich verboten ist, ermächtigen die Vorschriften die Strafverfolgungsbehörden dazu, sowohl polizeiinterne als auch -externe Dateien miteinander abzugleichen, wenn diese Maßnahme die Aufklärung einer Straftat befördern kann. Die Befugnis umfasst die Anordnung der Datenübermittlung gegenüber Dritten – Behörden und Privaten – sowie die maschinelle Abgleichung dieser Daten untereinander und mit Daten, die zur Strafverfolgung erhoben wurden. In diesen Vorschriften sind die Aussonderungs-, Übermittlungs- und Unterstützungspflicht der speichernden Stelle mit geregelt.

Nach § 98a Abs. 1, Satz 1 StPO ist die Rasterfahndung ein maschinell-automatisierter Datenabgleich der personenbezogenen Daten von Personen, die bestimmte, auf den Täter vermutlich zutreffende Prüfungsmerkmale erfüllen, mit aus anderen Gründen an anderen Stellen gespeicherten Daten. Durch diesen Abgleich sollen Nichtverdächtige ausgeschlossen oder Personen festgestellt werden, die weitere für die Ermittlungen bedeutsame Prüfungsmerkmale erfüllen. Mit Hilfe dieser Ermittlungsmethode, der sog. Rasterfahndung, bei der die Möglichkeit der automatisierten Datenverarbeitung für Zwecke der Strafverfolgung genutzt wird, sollen Hinweise und Spuren gefunden werden, die nach kriminalistischer Erfahrung

191 Das beruht auf der damaligen Erwägung, dass Datenverarbeitungsvorgänge ohne Grundrechtsrelevanz sind (*Ermisch*, Fahndung und Datenschutz – aus der Sicht der Polizei, in: Bundeskriminalamt (Hrsg.), Möglichkeiten und Grenzen der Fahndung, Vortragsreihe Bd. 25, 63 (63, 67)).

zur Aufklärung einer Straftat beitragen können. Diese werden dann auf herkömmliche Weise abgeklärt.[192]

Die elektronische Datenverarbeitung zu Zwecken der Fahndung gewinnt an Bedeutung. Damit einhergehend steigt auch das Bedürfnis nach dem Schutz personenbezogener Daten im Rahmen der Fahndung. Bei jeder Form von Rasterfahndung werden regelmäßig Daten von den Strafverfolgungsbehörden auf deren Ersuchen und zu deren Zweckverfolgung verarbeitet, ohne dass die Betroffenen von diesem Vorgang Kenntnis erhalten. Die heimliche Datenverarbeitung hemmt die Ausübung des Rechts auf informationelle Selbstbestimmung und kann einen psychischen Anpassungsdruck in Richtung einer möglichst unauffälligen Verhaltensweise auslösen. Dieser würde nach der Auffassung des Bundesverfassungsgerichts nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl. Diese Gefahr verschärft die Möglichkeit einer Persönlichkeitserfassung aufgrund der Verarbeitungsgeschwindigkeit sowie der Verknüpfungs- und Speichermöglichkeiten, über die die moderne Informationsverarbeitungstechnologie verfügt. Die Verknüpfung mehrerer Daten, deren Speicherzwecke unterschiedlich sind, würde die Bürger angesichts der für sie nicht durchschaubaren Möglichkeiten der elektronischen Datenverarbeitung verunsichern und stellt somit einen Eingriff in das Recht auf informationelle Selbstbestimmung dar. Angesichts des Umstands, dass in die Massenfahndungsmethode der Rasterfahndung typischerweise eine Vielzahl von unverdächtigen Dritten einbezogen werden, ist die Gefahr eines Missbrauchs der Staatsgewalt nicht von der Hand zu weisen.

Es ist daher zu klären, ob die Ermittlungsmethode der Rasterfahndung das Recht auf informationelle Selbstbestimmung ausreichend schützt, also ob die verfahrensrechtlichen Vorkehrungen für die Durchführung und die Organisation den vom Bundesverfassungsgericht im Volkszählungsurteil aufgestellten Grundsätzen zur Einschränkung des Rechts auf informationelle Selbstbestimmung genügen.[193] Dafür soll im Folgenden die gesetzli-

192 BT-Drs. 12/989, S. 36.

193 Siehe auch *Pehl*, Die Implementation der Rasterfahndung – eine empirische Untersuchung zur Anwendung, Umsetzung und Wirkung der gesetzlichen Regelungen zur operativen Informationserhebung durch Rasterfahndung, 2008, Berlin. Pehl zielt im Hinblick auf die Verfassungsmäßigkeit der Rasterfahndung darauf ab, eine empirische Datenbasis für zukünftige rechtspolitische Diskussionen und Entscheidungen zu schaffen, damit Implementations- und Evaluationsfragestellungen im Zusammenhang mit der Rasterfahndung auf der Basis empirischer Befunde diskutiert werden können.

che Gestaltung der Ermittlungsmethode „Rasterfahndung" konkret analysiert werden. Genauer gesagt soll untersucht werden, welche Daten unter welchen Bedingungen zu Zwecken der Rasterfahndung genutzt werden dürfen, wie lange die Daten gespeichert werden, ob eine Löschungspflicht statuiert wird, und wenn ja, wann die Daten konkret gelöscht werden sollen.

1. Organisationsstruktur

Die StPO differenziert zwischen dem Abgleich von polizeiinternen Dateien – dem üblichen polizeilichen Datenabgleich, das heißt dem Abgleich von Dateien, die der Polizei bereits zur Verfügung stehen (§ 98c StPO) – und polizeiexternen Dateien, die aus anderen Gründen an anderen Stellen gespeichert sind (Rasterfahndung im eigentlichen Sinn, §§ 98a und 98b StPO). Nach § 98c StPO dürfen also zur Aufklärung einer Straftat personenbezogene Daten aus einem Strafverfahren mit anderen zur Strafverfolgung oder Strafvollstreckung oder zur Gefahrenabwehr gespeicherten Daten maschinell abgeglichen werden. Die Vorschrift regelt jedoch keine Rasterfahndung wie in § 98a, sondern nur die Befugnis zum Abgleich bereits bei der Gefahrenabwehr oder bei der Strafverfolgung oder Strafvollstreckung gewonnener personenbezogener Daten aus einem Strafverfahren. § 98a Abs. 1 und 2 erlaubt den automatisierten Abgleich von Daten nur durch die Strafverfolgungsbehörden. Dabei ist die öffentliche oder private Stelle, bei der die für den Abgleich benötigten Daten gespeichert sind, verpflichtet, diese Daten aus ihrem Datenbestand auszusondern und den Strafverfolgungsbehörden zu übermitteln. Die speichernde Stelle ist nur dazu verpflichtet, die bereits bei ihr gespeicherten Daten zu übermitteln, aber sie darf nicht erst auf Anfrage der Staatsanwaltschaft Daten zum Zweck der Rasterfahndung erheben. Die Übermittlungspflicht beschränkt sich auf die Übermittlung der für den Datenabgleich erforderlichen Daten. Darüber hinaus hat die speichernde Stelle auf Anforderung der Staatsanwaltschaft die Abgleichstelle zu unterstützen. Der Abgleich darf sowohl zur Aufklärung einer Straftat als auch zur Ermittlung des Aufenthaltsortes einer Person erfolgen, nach der zu Zwecken eines Strafverfahrens gefahndet werden soll. Hierbei sind keine verfahrensrechtlichen Schutzvorkehrungen wie Richtervorbehalt, Straftatenkatalog oder Subsidiaritätsklausel vorgesehen und es bestehen auch keine Regelungen zur Rückgabe und Vernichtung von Daten, zur nachträglichen Unterrichtung der Betroffenen oder zur Mitwirkung von Datenschutzbeauftragten.

Nach § 98a StPO werden bereits vorhandene, personenbezogene Datenbestände, die von öffentlichen und nichtöffentlichen Stellen, die keine Strafverfolgungsbehörden sind, für andere Zwecke als die Strafverfolgung erhoben wurden, computergestützt nach bestimmten tätertypischen Prüfungsmerkmalen (Rastern) überprüft und abgeglichen. Durch die Rasterfahndung sollen Nichtverdächtige ausgeschlossen (negative Rasterfahndung) oder Personen festgestellt werden, die weitere für die Ermittlungen bedeutsame Prüfungsmerkmale erfüllen (positive Rasterfahndung). Der Unterschied zwischen der negativen und der positiven Rasterfahndung liegt darin, dass bei ersterer ein einzelner von den Strafverfolgungsbehörden zu untersuchender Datenbestand durch Löschen von Personaldaten, die auf den Täter nicht zutreffen, auf einen Restbestand reduziert wird, während bei letzterer polizeilicher Einblick in eine Vielzahl von Dateien genommen wird.

Die Rasterfahndungsmethoden können nach der unterschiedlichen Eingriffsintensität unterteilt vorgestellt werden: die positive Rasterfahndung nach unbekannten Tätern, die negative Rasterfahndung mit einer Fremddatei als Ausgangsdatei und die negative Rasterfahndung mit einer Ausgangsdatei, die zu Strafverfolgungszwecken angelegt ist. Jede Form von Rasterfahndung hat eine jeweils unterschiedliche Eingriffsintensität. Bei der positiven Rasterfahndung führen nicht die Strafverfolgungsbehörden, sondern regelmäßig verschiedene Behörden und private Einrichtungen Suchläufe in den eigenen Dateien für Strafverfolgungszwecke durch. Nach diesen Suchläufen wird ein gefundener Datensatz in einer gesonderten Ergebnisdatei abgespeichert. Nur die Ergebnisdateien werden von den Strafverfolgungsbehörden eingesehen und miteinander oder mit Dateien abgeglichen, die bereits zu Strafverfolgungszwecken angelegt sind. Dabei ist grundrechtlich nicht nur zu bedenken, dass die auf dem Ergebnisband abgespeicherten Daten eine Kontextänderung erfahren, sondern auch, dass die von verschiedenen Behörden und privaten Einrichtungen durchgeführten Suchläufe in keinem Zusammenhang mit der eigentlichen Zwecksetzung der Datenspeicherung stehen. Außerdem besteht bei der Rasterfahndung für die herausgerasterten Personen die Gefahr, dass deren personenbezogene Daten zu einem partiellen oder vollständigen Persönlichkeitsbild zusammengefügt werden, sogar ohne Wissen der Betroffenen. Diese Möglichkeit löst einen psychischen Anpassungsdruck in Richtung der als „normal“ vermuteten Verhaltensmuster aus.

Bei der negativen Rasterfahndung gleichen die Strafverfolgungsbehörden demgegenüber die verschiedenen Dateien ab, um Personendaten aus einer Fremd- oder einer Ausgangsdatei, die zu Strafverfolgungszwecken

angelegt ist, zu löschen. Die Strafverfolgungsbehörden sehen nur die Ausgangsdatei ein, weil die Abgleichdateien beim Abgleich lediglich dazu genutzt werden, Daten aus dem Ausgangsdatenbestand zu löschen. Es entsteht hier jedoch eine Missbrauchsgefahr, weil die Abgleichdateien immerhin den Strafverfolgungsbehörden zur Verfügung gestellt werden. Bei der negativen Rasterfahndung mit einer Fremddatei als Ausgangsdatei wird die Ausgangsdatei aus ihrem ursprünglichen Kontext herausgelöst und in den polizeilichen Fahndungskontext überführt, während bei der negativen Rasterfahndung mit einer Ausgangsdatei, die zu Strafverfolgungszwecken angelegt ist, die Ausgangsdatei keine Zweckänderung erfährt.

Wenn eine Rasterfahndungsanordnung seitens des Ermittlungsrichters ergangen ist, läuft die Rasterfahndung in folgenden Schritten ab:

Zunächst wird eine Suchanfrage zur Recherche in den Datenbeständen öffentlicher und nichtöffentlicher Stellen mit Hilfe von Rastern für den konkreten Einzelfall (§ 98a Abs. 1 S. 5 StPO) unter Verwendung logischer Verknüpfungen zur Erstellung eines bestimmten Verdächtigenprofils formuliert. Anhand dieser Suchanfrage werden die Datenbestände nach bestimmten zuvor aufgestellten Kriterien durchsucht. Diejenigen Informationen, die mit der Suchanfrage übereinstimmen (Treffer), werden selektiert und in eine separate Datei (Report) ausgesondert und dort gespeichert. Bereits in diesem Stadium sind die Daten derjenigen, die mit den Rastern nicht übereinstimmen, im Wege der negativen Rasterfahndung auszufiltern. Übrig bleiben die Daten derer, die im Wege der positiven Rasterfahndung unter das Raster fallen und somit dem Verdächtigenprofil entsprechen. Die gesonderte Datei wird durch den Gewahrsamsinhaber an die Strafverfolgungsbehörden übermittelt. Nach § 98a Abs. 2 StPO ist die speichernde Stelle dazu verpflichtet, die erforderlichen Daten auszusondern und den Strafverfolgungsbehörden zu übermitteln. Über die Aussonderungs- und Herausgabepflicht hinaus hat die Speicherstelle auf Anforderung der Staatsanwaltschaft die Abgleichstelle zu unterstützen. Als Unterstützungshandlung gilt hierbei jede geeignete und zumutbare Hilfe, wobei insbesondere Bedienungshinweise, Passwortfreigabe, aktive Mitwirkung von Personal sowie die Nutzung von Programmen und Hardware der Speicherstelle in Betracht kommen.[194] Die so ausgesonderten und übermittelten Daten werden sodann bei den Strafverfolgungsbehörden mit anderen Daten maschinell abgeglichen. Beim Abgleich werden anhand (weiterer) Raster entweder positiv Personen festgestellt, die diesen Rastern entsprechen, oder negativ die Personen ausgesondert, die zwar das

194 *Greven*, KK-StPO, § 98a Rn. 27.

Verdächtigenprofil, nicht aber die Raster erfüllen. Sollte die durchgeführte Rasterung einen Tatverdacht ergeben, da einzelne Personen die Raster erfüllen, wird diesem mit den üblichen Ermittlungsmethoden weiter nachgegangen.

2. Abgleichbare Daten

Der Gesetzgeber hat bei der gesetzlichen Formulierung der Rasterfahndung die Art, den Inhalt und den Umfang der zu verwendenden Daten nicht näher umschrieben, sondern vielmehr den unpräzisen Begriff „personenbezogene Daten" gewählt. Diese Daten können von verschiedenen Speicherstellen angefordert und mit anderen Daten maschinell abgeglichen werden können. Der Gesetzgeber scheint also eine pauschale Erlaubnis zur Verarbeitung personenbezogener Daten zu geben.[195]

Die unpräzise Formulierung dürfte auf der Tatsache beruhen, dass es schwierig ist, bereits in der gesetzlichen Regelung zu beurteilen, welche Informationen über eine Person im Einzelfall aufklärungsrelevant sein können. Angesichts des Risikos einer zu extensiven Auslegung des Begriffs „personenbezogene Daten" und der Gefahr, dass mangels der Eingrenzung der personenbezogenen Daten durch die Verwendung von sensiblen Daten bzw. die Verknüpfung von an sich betrachtet vielleicht weniger sensibel erscheinenden Daten Persönlichkeitsbilder entstehen, ist ein Bemühen um Normenklarheit erforderlich.

3. Verwendung des Datenabgleiches

Angesichts der Gefahren, die mit einer Rasterfahndung verbunden sind, wird zweierlei Einschränkungen Rechnung getragen: zum einen der Einschränkung auf Straftaten von erheblicher Bedeutung, die durch den typisierenden Katalog ergänzt werden, und zum anderen dem Richtervorbehalt.

---

195 Vgl. die von *Riegel* und *Rogall* vorgeschlagenen Entwürfe: Die Übermittlung von Daten zu Rasterfahndungszwecken soll auf Namen, Anschrift und Geburtsdatum der betreffenden Personen beschränkt werden, mit Ergänzung um die Prüfungsmerkmale (*Riegel*, Rechtsprobleme der Rasterfahndung, ZRP 1980, 300, 306; *Rogall*, Moderne Fahndungsmethoden im Lichte eines gewandelten Grundrechtsverständnisses, GA 1985, 1, 20).

Eine besondere Fahndungsmethode der Polizei unter Einsatz von Computertechnologie, nämlich die Rasterfahndung mit polizeiexternen Dateien, darf nur bei Vorliegen zureichender tatsächlicher Anhaltspunkte für bestimmte Delikte eingesetzt werden, die in § 98a Abs. 1 Satz 1 StPO aufgeführt werden. Dies sind Straftaten „von erheblicher Bedeutung

1. auf dem Gebiet des unerlaubten Betäubungsmittel- oder Waffenverkehrs, der Geld- oder Wertzeichenfälschung,
2. auf dem Gebiet des Staatsschutzes (§§ 74a, 120 GVG),
3. auf dem Gebiet der gemeingefährlichen Straftaten,
4. gegen Leib oder Leben, die sexuelle Selbstbestimmung oder die persönliche Freiheit,
5. erwerbs- oder bandenmäßig oder
6. von einem Bandenmitglied oder in anderer Weise organisiert" begangen werden.

Mit Blick auf die Katalogtaten werden jedoch weder die den einzelnen Straftaten zuzuordnenden Gesetzesparagraphen bezeichnet, noch sind die gemeinsamen Merkmale der bezeichneten Straftaten erkennbar.[196] Außerdem ist die Bezeichnung „von erheblicher Bedeutung" problematisch. Denn was eine Straftat von erheblicher Bedeutung ist, lässt sich nur schwer bestimmen, und ob dieses Merkmal erfüllt ist, wird sich vielfach erst im Lauf der Ermittlungen ergeben. Diese Gesetzgebungstechnik oder die dabei verwendeten Begriffe könnten somit der Eingriffsintensität der Rasterfahndung nicht entsprechen und darüber hinaus gegen den Grundsatz der Normenklarheit verstoßen.

Die Rasterfahndung mit polizeiexternen Dateien darf nur durch das Gericht – bei Gefahr im Verzug auch durch die Staatsanwaltschaft – und nur dann angeordnet werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters durch andere Maßnahmen erheblich weniger erfolgversprechend oder wesentlich erschwert wäre. Die staatsanwaltschaftliche Eilanordnung bedarf der unverzüglichen richterlichen Bestätigung. Wird die Anordnung nicht binnen drei Tagen von dem Richter bestätigt, so tritt sie außer Kraft (§ 98b Abs. 1 S. 3 StPO). Der Richtervorbehalt ist eine wichtige verfahrensrechtliche Vorkehrung, um die Rechtsschutz- und Kontrollfunktion für Grundrechtseingriffsmaßnahmen auszuführen. Die Einschränkung von Grundrechten erfordern

196 *Siebrecht*, Rasterfahndung – eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, S. 115.

ein zwingendes Bedürfnis. Dieses ist bei einer Rasterfahndung jedoch nicht erkennbar. Eine Rasterfahndung benötigt eine gewisse Vorlaufzeit, weil die verschiedenen Speicherstellen daran teilnehmen müssen. Der Fall eines besonderen Eilbedürfnisses, das die Einholung einer richterlichen Entscheidung nicht zulassen würde, ist daher schwer vorstellbar.[197] Die richterliche Bestätigung innerhalb von drei Tagen ist ebenfalls bedenklich. Denn die Tatsache, dass die richterliche Bestätigung ausbleibt oder versagt wird, macht die Übermittlung und den Abgleich von Daten aufgrund staatsanwaltschaftlicher Anordnung nicht rechtswidrig. Dann entsteht das Problem der Verwertbarkeit der durch die Maßnahme erlangten Erkenntnisse. Eine Lösung dieses Problems kann nicht im Gesetz gefunden werden. Bestenfalls kann das Heranziehen der erlangten Beweismittel zur Beweisführung vom Tatrichter im Hauptverfahren abgelehnt werden.[198]

4. Aufbewahrungsdauer der Daten

Gemäß § 98b Abs. 3 Satz 1 StPO sind die erhaltenen Datenträger nach Beendigung des Abgleichs unverzüglich an die betreffenden Speicherstellen zurückzugeben. Personenbezogene Daten, die auf andere Datenträger übertragen wurden, sind unverzüglich zu löschen, sobald sie für das Strafverfahren nicht mehr benötigt werden (§ 98b Abs. 3 Satz 2 StPO). Der Grund dafür, dass für das Löschen übertragener Daten ein späterer Zeitpunkt als für die Rückgabe der Datenträger gilt, ist der, dass die übertragenen Daten möglicherweise zur Beweisführung benötigt werden.[199] Durch die Löschung oder Rückgabe von Daten wird verhindert, dass Daten auf Vorrat gesammelt werden. Daher sind die Daten auf den erhaltenen Datenträgern unverzüglich, also *ohne eine nicht durch die Sachlage begründete Verzögerung*,[200] sofort nach der Beendigung des Abgleichs zurückzugeben und die Daten auf den übertragenen Datenträgern unver-

197 *Siebrecht*, Rasterfahndung – eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, S. 133.

198 *Schnarr*, Zur Verknüpfung von Richtervorbehalt, staatsanwaltlicher Eilanordnung und richterlicher Bestätigung, NStZ 1991, 209, 215.

199 Vgl. *Siebrecht*, Rasterfahndung – eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, S. 135 f. m. w. N.

200 *Schmitt*, Strafprozessordnung, § 98b Rn. 6 unter Hinweis auf § 25 Rn. 8; vgl. die Legaldefinition in § 121 BGB: „ohne schuldhaftes Zögern".

züglich zu löschen, sobald sie für das Strafverfahren nicht mehr benötigt werden. Die Daten sind damit spätestens mit rechtskräftigem Abschluss des Strafverfahrens zu löschen.[201] Eine Aufbewahrung über den gesetzlich normierten Zeitpunkt hinaus ist deshalb rechtswidrig, weil die weitere Aufbewahrung der Datenträger eine Aufrechterhaltung des Eingriffs in das informationelle Selbstbestimmungsrecht ohne die verfassungsrechtlich erforderliche gesetzliche Grundlage darstellt. Die Löschungspflicht gemäß § 98b Abs. 3 Satz 2 StPO ist gerade vor dem Hintergrund der Gefahren einer unbegrenzten Speicherung, Verwendung und Weitergabe von elektronischen Daten, die mit der modernen Datenverarbeitung verbunden sind, von besonderer Bedeutung.

Darüber hinaus ist zu bedenken, dass es keine Löschungs- oder Vernichtungsvorschrift für Daten gibt, die zwar aufgrund einer staatsanwaltschaftlichen Eilanordnung erlangt worden sind, danach jedoch gerichtlich nicht bestätigt wurden und damit außer Kraft treten.

5. Mitteilungspflicht

Bei der Rasterfahndung sind zwei Arten der Mitteilungspflicht mit geregelt: zum einen die Benachrichtigung der Betroffenen und zum anderen die Unterrichtung der für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz zuständigen Stelle.

§ 101 Abs. 4 Satz 1 Nr. 1 StPO statuiert die Pflicht zur nachträglichen Unterrichtung der Personen, gegen die nach Abgleich der Daten weitere Ermittlungen geführt wurden. Die weiteren Ermittlungen in diesem Sinn sind Ermittlungshandlungen herkömmlicher Art, wie die Vernehmung dieser Personen, Durchsuchungen, Nachforschungen in ihrem Umfeld oder die bloße Einholung von Auskünften über sie.[202] Somit fallen alle

201 Dagegen wird zum Teil die Auffassung vertreten, dass das Datenmaterial auch nach Urteilsrechtskraft für ein Wiederaufnahmeverfahren benötigt werden könnte und deshalb nicht zu vernichten ist(*Greven*, KK-StPO, § 98b Rn. 8 unter Hinweis auf *Schmitt*, Strafprozessordnung, § 101 Rn. 27). Dem ist jedoch entgegenzuhalten, dass allein die abstrakte Möglichkeit der Nützlichkeit von Daten in einem Wiederaufnahmeverfahren keine zeitlich unbegrenzte Aufrechterhaltung des Eingriffs in das Grundrecht auf informationelle Selbstbestimmung rechtfertigt (*Siebrecht*, Rasterfahndung – eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, S. 136 f.).

202 BT-Drs. 12/989, S. 38; *Erb*, LR-StPO, § 163d Rn. 81.

übrigen Betroffenen, deren personenbezogene Daten ebenfalls in die Rasterfahndung einbezogen waren, aus der Benachrichtigungspflicht heraus. Das beruht auf der Tatsache, dass Personen, die im Zuge einer Rasterfahndung von den Informationsverarbeitungsvorgängen betroffen sind, mit unterschiedlicher Intensität in ihrem Recht auf informationelle Selbstbestimmung beeinträchtigt werden. Diejenigen, die als Merkmalsträger nach mehreren Suchläufen herausgerastert wurden, sind stärker betroffen als diejenigen, deren Daten sich auf Datenträgern befinden, ohne zur Kenntnis genommen zu werden. Denn erst für denjenigen, der aus Datenträgern herausgefiltert wird, kommt es unmittelbar zu einer Gefährdung, während für alle übrigen nur die mittelbare Gefahr besteht, möglicherweise zur Kenntnis genommen zu werden.

Aber die personelle Beschränkung der Benachrichtigungspflicht auf diejenigen Merkmalsträger, gegen die weitere Ermittlungen geführt worden sind, geht zu weit, weil die Benachrichtigungspflicht nicht durch die Rasterfahndung an sich ausgelöst wird, sondern erst durch die dadurch veranlasste Vornahme weiterer Ermittlungen gegen diese Personen. Darüber hinaus entspricht die Beschränkung auch nicht dem Gebot des effektiven Rechtsschutzes. Für einen effektiven Rechtsschutz müssen die Bürger grundsätzlich Kenntnis davon haben, über welche sie betreffenden Informationen staatliche Stellen verfügen. In den Bereichen, in denen die Datenverarbeitung nicht offen aufgrund freiwillig gemachter Angaben betrieben wird, hängt diese Kenntnis ausschließlich von der Auskunftserteilung ab. Aus diesem Grund wird die Regelung der Benachrichtigungspflicht gefordert.

Die nachträgliche Benachrichtigung sollte daher grundsätzlich alle herausgerasterten Merkmalsträger einschließen. Sie sollte außerdem inhaltlich Folgendes enthalten: zunächst die Tatsache, dass eine Rasterfahndung angeordnet und durchgeführt wurde. Des Weiteren ist mitzuteilen, bei welcher Speicherstelle Daten ausgesondert, welche Prüfungsmerkmale gerastert wurden und welche Stelle im Besitz der Daten war oder noch ist.[203]

Die Benachrichtigung unterbleibt oder wird zurückgestellt, wenn ihr überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen oder sie den Untersuchungszweck, das Leben, die körperliche Unversehrtheit und die persönliche Freiheit einer Person und bedeutende

203 *Siebrecht*, Rasterfahndung – eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, S. 141; *Paa*, Der Zugriff der Strafverfolgungsbehörden auf das Private im Kampf gegen schwere Kriminalität, S. 217 f.

Vermögenswerte gefährden könnte. Die Dauer der Benachrichtigungszurückstellung bestimmt das Gericht. Es kann dem endgültigen Absehen von der Benachrichtigung zustimmen, wenn die Voraussetzungen für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden. Die Benachrichtigung wird nachgeholt, sobald die Einschränkungsgründe wegfallen (§ 101 Abs. 4, 5 und 6 StPO).

Darüber hinaus ist gemäß § 98b Abs. 4 StPO nach Beendigung einer Maßnahme nach § 98a die Stelle zu unterrichten, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständig ist. Denn der Einzelne kann überaus komplexe administrative Zusammenhänge sowie hochtechnische Verarbeitungsprozesse nur schwer durchschauen.[204] Aber die nachträgliche Kontrolle der zuständigen Stelle ist nicht umfangreich und reicht daher nicht aus. Zur effektiven Kontrolle des Datenschutzes sollten Vorabunterrichtung, Beratung und begleitende Kontrolle vorausgesetzt werden.[205]

III. Vorratsdatenspeicherung

1. Geschichtlicher Hintergrund

§ 12 FAG[206] regelte die Möglichkeit des Auskunftsverlangens über den Fernmeldeverkehr durch den Richter und bei Gefahr im Verzug auch

204 *Simitis*, Die informationelle Selbstbestimmung – Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, 398, 403.

205 *Siebrecht*, Rasterfahndung – eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, S. 143.

206 Das Gesetz über Fernmeldeanlagen (FAG) wurde erstmals als Neubekanntmachung des Gesetzes über das Telegraphenwesen des Deutschen Reichs herausgegeben, 6. April 1892 (RGBl. S. 467), die weitere Neubekanntmachung vom 3. Juli 1989 (BGBl. I S. 1455). Zum 1. Januar 1998 trat das FAG überwiegend und zum 1. Januar 2002 vollends außer Kraft. Nachfolgeregelungen sind vor allem im Telekommunikationsgesetz vom 25. Juli 1996 (BGBl. I S. 1120) enthalten.

durch die Staatsanwaltschaft.[207] Dabei legte § 5 TDSV[208] fest, welche Verbindungsdaten von Diensteanbietern – z. B. der Deutschen Telekom – gespeichert werden durften. Die folgenden Verbindungsdaten durften erhoben und verarbeitet werden: die Rufnummer oder die Kennung des anrufenden und des angerufenen Anschlusses, die personenbezogene Berechtigungskennung, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen und Kartenanschlüssen auch die Standortkennung (§ 5 Abs. 1 Nr. 1); Beginn und Ende der jeweiligen Verbindung nach Datum und Uhrzeit und, soweit die Entgelte davon abhingen, die übermittelten Datenmengen (§ 5 Abs. 1 Nr. 2); die vom Kunden in Anspruch genommene Telekommunikationsdienstleistung (§ 5 Abs. 1 Nr. 3); die Endpunkte von festgeschalteten Verbindungen sowie deren Beginn und Ende nach Datum und Uhrzeit (§ 5 Abs. 1 Nr. 4).[209] Ein Problem lag hierbei darin, dass eine Anordnung zur Auskunft über diese Daten erfolglos sein konnte, da die Daten nur für einen durch das Gesetz nicht näher spezifizierten Zeitraum aufbewahrt wurden. Das heißt, die Strafverfolgungsbehörden konnten nur auf die zum Zeitpunkt der Erhebung noch beim Telekommunikationsanbieter gespeicherten Daten zurückgreifen. Da die Speicherdauer jedoch bei jedem Anbieter unterschiedlich war, war es dem Zufall überlassen, ob die Verkehrsdaten zum Zeitpunkt des Zugriffs noch vorhanden waren oder nicht. Dies konnte zu Schwierigkeiten bei der Strafverfolgung und gegebenenfalls zu erfolglosen Ermittlungen führen.

In diesem Zusammenhang hat der Wunsch der Strafverfolgungsbehörden nach Einführung einer Speicherung von Telekommunikationsdaten für Strafverfolgungszwecke auf EU-Ebene eine lange Geschichte. Diese Daten umfassen Verkehrsdaten, die nicht zu Abrechnungszwecken gespeichert werden müssen, Standortdaten sowie eindeutige Geräteidentifikationen. Die Speicherfrist geht dabei deutlich über die für reine Vertragszwecke zulässige Dauer hinaus, und die Speicherung wird weder durch Ver-

207 § 12 FAG: In strafrechtlichen Untersuchungen kann der Richter und bei Gefahr im Verzug auch die Staatsanwaltschaft Auskunft über den Fernmeldeverkehr verlangen, wenn die Mitteilungen an den Beschuldigten gerichtet waren oder wenn Tatsachen vorliegen, aus denen zu schließen ist, dass die Mitteilungen von dem Beschuldigten herrührten oder für ihn bestimmt waren und dass die Auskunft für die Untersuchung Bedeutung hat.

208 Verordnung über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM (Telekom-Datenschutzverordnung) vom 24. Juni 1991, BGBl. 1991, I. S. 1391.

209 Die Vorschrift wurde später durch § 96 TKG ersetzt.

tragszwecke noch durch einen bestimmten Tatverdacht veranlasst. Sowohl in Deutschland als auch auf europäischer Ebene gab es seit langem Bemühungen, die Vorratsdatenspeicherung von Kommunikationsdaten einzuführen; alle Versuche waren jedoch gescheitert. Bereits im Jahre 1996 wurde in Deutschland der erste Versuch unternommen, eine Mindestspeicherfrist von Telekommunikationsdaten zu etablieren. Damit sollte vermieden werden, dass die von Strafverfolgungsbehörden angeforderten Daten nicht mehr vorhanden waren.[210] Dieser Versuch einer Gesetzgebung scheiterte an der Ablehnung der damaligen Bundesregierung, nach deren Auffassung eine Mindestspeicherfrist den verfassungsrechtlichen Geboten der Verhältnismäßigkeit, der Erforderlichkeit und der Zweckbindung widersprochen hätte.[211] Einen weiteren nennenswerten Versuch, eine Vorratsdatenspeicherung zur Diskussion zu stellen, gab es im Jahre 2000 im Rahmen der Innenministerkonferenz. Die Forderung nach Einführung der Vorratsdatenspeicherung wurde allerdings von den Datenschutzbeauftragten scharf kritisiert und anschließend abgelehnt.[212]

Die Einführung der Vorratsdatenspeicherung in Deutschland begann daher nicht auf nationaler, sondern auf europäischer Ebene. Als Reaktion auf die Zuganschläge am 11. März 2004 in Madrid und vor allem auf die Bombenanschläge vom 7. Juli 2005 auf U-Bahnen und einen Bus in London wurde nach dem bis zu diesem Zeitpunkt kürzesten Rechtsetzungsverfahren am 15. März 2006 die Richtlinie 2006/24/EG (Vorratsdatenspeicherungsrichtlinie) verabschiedet; sie trat zum 3. Mai 2006 in Kraft.[213] Gemäß Art. 15 Vorratsdatenspeicherungsrichtlinie waren die Mitgliedstaaten dazu verpflichtet, die Richtlinie bis zum 15. September 2007 und bezüglich der Internetdienste bis zum 15. März 2009 in nationales Recht umzusetzen. Die Richtlinie wurde demgemäß in Deutschland mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen vom 21. Dezember 2007

210 BT-Drs. 13/4438, S. 23.
211 BT-Drs. 13/4438, S. 39.
212 *Moser-Knierim*, Vorratsdatenspeicherung – Zwischen Überwachungsstaat und Terror-abwehr, S. 150.
213 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. EU Nr. L 105, S. 54–60.

in nationales Recht umgesetzt.[214] Hierbei wurden jedoch wiederkehrend verfassungsrechtliche Bedenken gegen die Vorratsdatenspeicherung geäußert, aufgrund derer es in der Folge zu einer rechtlichen Diskussion in Deutschland und auf europäischer Ebene kam. In der Folge wurde die Vorratsdatenspeicherung sowohl vom EuGH als auch vom Bundesverfassungsgericht jeweils für ungültig[215] oder für verfassungswidrig und nichtig erklärt.[216] Daraufhin wurde im Oktober 2014 ein neues Gesetz zur Vorratsdatenspeicherung in Deutschland verabschiedet, das am 18. Dezember 2015 in Kraft trat.[217] Doch selbst gegen das neue Gesetz, das den Anforderungen des Bundesverfassungsgerichts genügte, wurde erneut Verfassungsbeschwerde eingereicht.

a) Die Vorratsdatenspeicherungsrichtlinie auf europäischer Ebene

aa) Entstehungsgeschichte der Richtlinie

Das Recht auf Privatsphäre ist auf europäischer Ebene sowohl in der Konvention zum Schutz der Menschenrechte und Grundfreiheiten (EMRK) als auch in Verträgen und Gesetzgebungen der EU verankert. Der Europäische Gerichtshof für Menschenrechte (EGMR) hat den Geltungsbereich des Rechts auf Privatsphäre um die Feststellung erweitert, dass Artikel 8 der EMRK auch ein Recht auf Datenschutz gewährleistet, obwohl der EGMR im Rahmen der EMRK häufig einen Ermessensspielraum für die Mitgliedstaaten eröffnete, wenn das Recht auf Privatsphäre mit nationalen Sicherheitsbedenken in Konflikt geriet. Auf Ebene der Europäischen Union sind die Privatsphäre und personenbezogene Daten durch Artikel 7 und 8 der Charta der Grundrechte der Europäischen Union (EU-Grundrechtecharta) geschützt. In Artikel 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV), der durch den 2009 in Kraft getretenen Vertrag von Lissabon[218] eingeführt wurde, wird erneut darauf hingewiesen, dass „jede Person das Recht auf Schutz der sie betreffenden personen-

214 Das Gesetz trat am 1. Januar 2008 in Kraft. Es wurde mit eindeutiger Mehrheit angenommen; vgl. dazu *Orantek*, Die Vorratsdatenspeicherung in Deutschland, NJ 2010, 193, 199.
215 EuGH, C-293/12, 8. April 2014.
216 BVerfGE 125, 260.
217 Verkündung BGBl. 2015 I S. 2218.
218 Der Vertrag von Lissabon zur Änderung des Vertrags über die Europäische Union und des Vertrags zur Gründung der Europäischen Gemeinschaft wurde

bezogenen Daten hat." Die Vorschrift ermächtigt den Unionsgesetzgeber zur Festlegung von Bestimmungen im Hinblick auf den Datenschutz. Die Einhaltung dieser Regeln unterliegt der Kontrolle unabhängiger Behörden.

Auf Ebene des Sekundärrechts wurde der Rahmen für den Datenschutz schrittweise durch die Richtlinie 95/46/EG zum Schutz der Privatsphäre von natürlichen Personen bei der Verarbeitung von personenbezogenen Daten und zum freien Datenverkehr (Datenschutzrichtlinie) geschaffen.[219] Diese beschreibt Mindeststandards für den Datenschutz, die in allen Mitgliedstaaten der EU durch nationale Gesetze sichergestellt werden müssen. Vor allem für die Verarbeitung personenbezogener Daten besteht eine Anforderung der Richtlinie darin, dass die Datenerhebung in Relation zu dem Zweck, zu dem sie unternommen wird,[220] verhältnismäßig sein muss und dass sie im Allgemeinen vorbehaltlich der Zustimmung des Betroffenen ist.[221] Die Verarbeitung sensibler Daten ist grundsätzlich verboten.[222] Die Betroffenen sollen gemäß der Richtlinie über die Verarbeitung ihrer Daten informiert werden[223] und sie sind ermächtigt, Zugang zu ihren Daten zu erhalten und bei Bedarf die Berichtigung, Sperrung oder Löschung ihrer Daten zu verlangen.[224] In diesem Zusammenhang wurden die Verordnung 45/2001/EG[225] – die anders als eine Richtlinie, die durch die nationalen Parlamente erst in innerstaatliche Gesetze umgesetzt werden muss, unmittelbar nach ihrer Verabschiedung in den Mitgliedstaaten Geltung hat – und die Richtlinie 2002/58/EG[226] nacheinander

---

im ABl. 2007/C 306/01 veröffentlicht, zuletzt durch Abdruck der konsolidierten Textfassungen im ABl. 2012/C 326/01 bekanntgemacht.

219 Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, 23. November 1995 (ABl. EG Nr. L 281 S. 31–50). Die Richtlinie wurde später durch die Verordnung (EU) 2016/679 am 25. Mai 2018 ersetzt.

220 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, Art. 6 (1).

221 a. a. O. Art. 7.

222 a. a. O. Art. 8 (1).

223 a. a. O. Art. 10.

224 a. a. O. Art. 12.

225 Verordnung (EG) Nr. 45/2001 vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr.

226 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der

erlassen. Letztere aktualisiert die Grundsätze der Datenschutzrichtlinie im Bereich der elektronischen Kommunikation und harmonisiert die Rechtsvorschriften der Mitgliedstaaten, um ein gleichwertiges Schutzniveau der Grundrechte und Grundfreiheiten sicherzustellen. Die Datenschutzrichtlinie wurde durch die Datenschutz-Grundverordnung ersetzt,[227] mit der die Regeln zur Verarbeitung personenbezogener Daten durch private Unternehmen und öffentliche Stellen EU-weit vereinheitlicht wurden. Dadurch soll der Schutz personenbezogener Daten innerhalb der EU sichergestellt sowie der freie Datenverkehr innerhalb des Europäischen Binnenmarktes gewährleistet werden.

Trotz dieser Bemühungen, die Regeln zur Verarbeitung personenbezogener Daten innerhalb der EU und ihrer Mitgliedstaaten zu vereinheitlichen, erlaubt der EU-Datenschutzrahmen bestimmte Ausnahmen, die die Mitgliedstaaten dazu ermächtigen, die in der Datenschutzrichtlinie angegebenen Rechte aus Gründen der nationalen Sicherheit einzuschränken. Aufgrund dieses außergewöhnlichen Ermessensspielraums führten einige EU-Mitgliedstaaten nach den Anschlägen vom 11. September 2001 Ausnahmen von den EU-Datenschutzvorschriften ein. Diese Fragmentierung der staatlichen Gesetzgebung hatte zur Folge, dass in unterschiedlichem Maße von den Datenschutzgrundsätzen der EU abgewichen und andere Regeln für die Vorratsdatenspeicherung von Daten durch Anbieter elektronischer Kommunikation festgelegt wurden. Mit dem Ziel, diese unterschiedlichen nationalen Gesetze miteinander in Einklang zu bringen, wurde im Jahr 2006 die Vorratsdatenspeicherungsrichtlinie[228] verabschiedet. Art. 1 Abs. 1 Vorratsdatenspeicherungsrichtlinie sieht die Verpflichtung der Mitgliedstaaten vor, bestimmte Daten, die von Anbietern öffentlich zugänglicher elektronischer Kommunikationsdienste oder von Betreibern ei-

---

Privatsphäre in der elektronischen Kommunikation, 31. Juli 2002 (ABl. EG Nr. L 201 S. 37–47).

227 Die Richtlinie wurde durch die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG am 25. Mai 2018 ersetzt, um eine umfassende Wahrung des Datenschutzes zu garantieren und Mitgliedstaaten stärker in die Pflicht zu nehmen. Die Verordnung 2016/679 (Datenschutz-Grundverordnung) trat am 24. Mai 2016 in Kraft.

228 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. EU Nr. L 105.

nes öffentlichen Kommunikationsnetzes erzeugt oder verarbeitet werden, auf Vorrat zu speichern. Das Ziel dieser Richtlinie ist zum einen die Harmonisierung einzelner mitgliedstaatlicher Vorschriften und zum anderen die Sicherstellung des Umstands, dass die Daten für die Ermittlung, Feststellung und Verfolgung schwerer Straftaten zur Verfügung stehen. Gemäß Art. 4 der Richtlinie müssen die Mitgliedstaaten in nationalem Recht die Voraussetzungen für den Zugang zu diesen Daten entsprechend dem Notwendigkeits- und dem Verhältnismäßigkeitsgrundsatz sowie im Einklang mit den einschlägigen Bestimmungen des Rechts der Europäischen Union oder des Völkerrechts und insbesondere der EMRK regeln. Die Richtlinie lässt den Mitgliedstaaten jedoch einen Ermessensspielraum bei der Festlegung der Bedingungen, die den Zugang zu den gespeicherten Daten rechtfertigen.

bb) Regelungen der Richtlinie

Die Richtlinie enthält 17 Vorschriften darüber, in welcher Weise konkrete Maßnahmen ergriffen werden dürfen. Als wesentlich können Art. 1, 5, 6, 7, 8 und 13 genannt werden. Art. 1 Vorratsdatenspeicherungsrichtlinie legt deutlich die Zielsetzung der Richtlinie fest, die zum einen in der Harmonisierung mitgliedstaatlicher Vorschriften über Vorratsdatenspeicherung und zum anderen in der Sicherstellung bestimmter Daten für die Ermittlung, Feststellung und Verfolgung schwerer Straftaten besteht. Hierbei kommen vornehmlich Terroranschläge und organisierte Kriminalität in Betracht. Darüber hinaus wird der Anwendungsbereich gemäß Art 1. Abs. 2 auf Verkehrs- und Standortdaten beschränkt; er erstreckt sich hingegen nicht auf den Inhalt elektronischer Nachrichtenübermittlungen einschließlich solcher Informationen, die mit Hilfe eines elektronischen Kommunikationsnetzes abgerufen werden. In Art. 5 Abs. 1 Vorratsdatenspeicherungsrichtlinie sind die zu speichernden Daten zunächst nach Verwendungszwecken enumerativ geordnet. Als Verwendungszwecke werden die folgenden genannt:

1. Rückverfolgung und Identifizierung der Quelle einer Nachricht
2. Identifizierung des Adressaten einer Nachricht
3. Bestimmung von Datum, Uhrzeit und Dauer einer Nachrichtenübermittlung
4. Bestimmung der Art einer Nachrichtenübermittlung

5. Bestimmung der Endeinrichtung oder der vorgeblichen Endeinrichtung von Benutzern
6. Bestimmung des Standorts mobiler Geräte

Die zu speichernden Daten, die diesen Verwendungszwecken dienen können, werden sodann abschließend aufgelistet. Erfasst werden dabei Verkehrs- und Standortdaten und alle damit in Zusammenhang stehenden Daten, die zur Feststellung des Teilnehmers oder Benutzers erforderlich sind.

Die oben genannten Daten sind gemäß Art. 6 Vorratsdatenspeicherungsrichtlinie mindestens sechs Monate und höchstens zwei Jahre ab dem Zeitpunkt der Kommunikation auf Vorrat zu speichern. Außerdem ist gemäß Art. 12 Vorratsdatenspeicherungsrichtlinie den Mitgliedstaaten die Möglichkeit beigemessen worden, die maximale Speicherfrist für einen begrenzten Zeitraum zu verlängern, sofern entsprechende Rechtfertigungsgründe vorliegen. Trifft die Kommission keine ausdrückliche Ablehnungsentscheidung, besteht für Mitgliedstaaten theoretisch der Raum, die Speicherfrist zwar für einen begrenzten, jedoch beliebigen Zeitraum zu verlängern. Unabhängig davon bleibt den Mitgliedstaaten bei der Wahl des Speicherzeitraums ein erheblicher Gestaltungsspielraum zwischen sechs und 24 Monaten. Um die Datensicherheit zu gewährleisten, verlangt Art. 7 Vorratsdatenspeicherungsrichtlinie ausdrücklich, dass geeignete technische und organisatorische Maßnahmen ergriffen werden sollen. Darüber hinaus ist auch die Löschpflicht nach dem Ablauf der Speicherfrist in Art. 7 Abs. d Vorratsdatenspeicherungsrichtlinie bestimmt.

Art. 8 Vorratsdatenspeicherungsrichtlinie fordert die Mitgliedstaaten dazu auf, die Daten so zu speichern, dass sie „unverzüglich an die zuständigen Behörden auf deren Anfrage hin weitergeleitet werden können". Die Bestimmung der dabei erforderlichen Maßnahmen (die zur Anfrage befugten staatlichen Stellen, die Anfrage- und Weitergabenvoraussetzungen sowie die konkreten Verfahren) ist den Mitgliedstaaten überlassen, soweit die Anforderungen der Notwendigkeit und der Verhältnismäßigkeit eingehalten werden. Art. 13 Vorratsdatenspeicherungsrichtlinie verpflichtet die Mitgliedstaaten zudem dazu, über Rechtsbehelfe, Haftung und Sanktionen die Umsetzung sicherzustellen, gewährt ihnen bei deren Konkretisierung allerdings einen weiten Gestaltungsspielraum.

cc) Das Urteil des Europäischen Gerichtshofs

Unmittelbar nach der Verabschiedung der Vorratsdatenspeicherungsrichtlinie wurde von Irland eine Klage vor dem Europäischen Gerichtshof angestrengt. Die Klage bezog sich auf die Wahl der Rechtsgrundlage (Art. 95 EGV a. F., jetzt Art. 114 AEUV); es handelte sich also um eine rein formelle Rechtsfrage. Eine mögliche Verletzung der Grundrechte als Folge von mit der Vorratsdatenspeicherungsrichtlinie verbundenen Eingriffen in das Recht auf Privatsphäre wurde hingegen nicht adressiert. Obwohl die formelle Frage der Richtlinie auch rechtswissenschaftlich umstritten war, wies der Europäische Gerichtshof die Klage mit der Begründung ab, dass sich die Regelungen zur Vorratsdatenspeicherung

„unmittelbar auf das Funktionieren des Binnenmarkts auswirken[229] und die Vorratsdatenspeicherungsrichtlinie Tätigkeiten regelt, die unabhängig von der Durchführung jeder eventuellen Maßnahme polizeilicher oder justizieller Zusammenarbeit in Strafsachen sind, damit sie die Diensteanbieter verpflichtet, die Daten, die im Zuge der Bereitstellung der betreffenden Kommunikationsdienste erzeugt oder verarbeitet wurden, auf Vorrat zu speichern".[230]

Die Frage nach der Vereinbarkeit der Richtlinie mit den EU-Grundrechten wurde erst in der Vorabentscheidung behandelt, in der der irische *High Court* und der österreichische Verfassungsgerichtshof dem EuGH die Frage vorlegten, ob die Vorratsdatenspeicherung mit den EU-Grundrechten vereinbar sei. Der EuGH erklärte mit seinem Urteil vom 8. April 2014 die Vorratsdatenspeicherungsrichtlinie (VDS-RL 2006/24/EG) für ungültig, da sie in die durch die Europäischen Grundrechtecharta garantierten Grundrechte auf Achtung des Privat- und Familienlebens (Art. 7 GRC) und auf Schutz der personenbezogenen Daten (Art. 8 GRC) eingreift[231] und der Unionsgesetzgeber dabei die Grenzen überschritten habe, die er zur Wahrung des Grundsatzes der Verhältnismäßigkeit einhalten müsse.[232] Nach der Rechtsprechung des EuGH ist der mit der Vorratsdatenspeicherungsrichtlinie verbundene Eingriff in die oben genannten Grundrechte von großem Ausmaß und als besonders schwerwiegend anzusehen.[233] Da der Schutz des Grundrechts auf Achtung des Privatlebens verlangt, dass sich

229 EuGH, C-301/06, 10.2.2009, Rn. 71.
230 EuGH, C-301/06, 10.2.2009, Rn. 82 f.
231 EuGH, C-293/12, 8.4.2014, Rn. 34 ff.
232 EuGH, C-293/12, 8.4.2014, Rn. 69.
233 EuGH, C-293/12, 8.4.2014, Rn. 37.

die Ausnahmen vom Schutz personenbezogener Daten auf das absolut Notwendige beschränken müssen,[234] wird von der Unionsregelung über die Vorratsdatenspeicherung gefordert, klare und präzise Regeln für ihre Tragweite und Anwendung festzulegen und einen wirksamen Schutz der personenbezogenen Daten vor Missbrauch, unberechtigtem Zugang und unberechtigter Nutzung sicherzustellen.[235]

In diesem Zusammenhang stellt die Vorratsdatenspeicherungsrichtlinie einen Eingriff in die in Art. 7 und 8 verankerten Grundrechte dar, der im Hinblick auf die Verhältnismäßigkeit deshalb nicht gerechtfertigt ist, weil in der Richtlinie keine Bestimmungen enthalten sind, die gewährleisten, dass sich der Eingriff tatsächlich auf das absolut Notwendige beschränkt.[236] Die Richtlinie verpflichtet erstens dazu, in umfassender Weise die Daten aller Personen anlassunabhängig zu speichern, die elektronische Kommunikationsdienste nutzen.[237] Zweitens sieht die Richtlinie für einen Zugriff auf die Daten keine Einschränkung auf konkrete schwere Straftaten vor.[238] Abschließend liegt ein weiteres Problem in der Dauer der Vorratsdatenspeicherung begründet. Denn nach der Richtlinie sind die Daten ohne eine Unterscheidung bezüglich der Datenkategorien nach Maßgabe ihres etwaigen Nutzens oder anhand der betroffenen Personen für einen Zeitraum von mindestens sechs Monaten auf Vorrat zu speichern.[239] Der EuGH erklärte die EU-Richtlinie 2006/24/EG über die Vorratsdatenspeicherung für ungültig, weil die darin vorgeschriebene Verpflichtung von Telekommunikationsanbietern, die Daten ihrer Nutzer zu speichern, nicht auf das Notwendige beschränkt gewesen sei.

Auf der Ebene der EU wird zwar immer wieder die Forderung nach einer Wiedereinführung der Vorratsdatenspeicherung laut, jedoch besteht bis heute keine wirksame Vorschrift zur Vorratsdatenspeicherung. Während die Vorratsdatenspeicherungsrichtlinie nicht mehr in Kraft ist, ihre Umsetzungsgesetze in den Mitgliedstatten jedoch noch bestehen, gab es im Jahr 2016 zwei Vorabentscheidungsverfahren des EuGH, in denen dem Gerichtshof die Frage vorgelegt wurde, ob die nationalen Regelungen mit der EU-Datenschutzrichtlinie für elektronische Kommunikation (2002/58/EG) mit der Grundrechtecharta vereinbar seien. Die Grundlage

234 EuGH, C-293/12, 8.4.2014, Rn. 52.
235 EuGH, C-293/12, 8.4.2014, Rn. 54.
236 EuGH, C-293/12, 8.4.2014, Rn. 65.
237 EuGH, C-293/12, 8.4.2014, Rn. 58.
238 EuGH, C-293/12, 8.4.2014, Rn. 60.
239 EuGH, C-293/12, 8.4.2014, Rn. 63.

hierfür waren entsprechende Verfahren in Schweden und Großbritannien. In beiden Ländern sind Telekommunikationsunternehmen dazu verpflichtet, umfangreiche Verkehrs- und Standortdaten ihrer Nutzer systematisch auf Vorrat zu speichern und den Behörden zur Verfügung zu stellen. In den Vorabentscheidungsverfahren stellte der EuGH klar, dass eine nationale Regelung, die eine allgemeine Speicherung von Daten ohne ausreichende begrenzende Kriterien zulässt, nicht mit dem Unionsrecht vereinbar sei.[240] Hiermit erteilte der EuGH einer allgemeinen Vorratsdatenspeicherung erneut eine deutliche Absage. Der Gerichtshof bestätigte zunächst, dass die Richtlinie 2002/58[241] den Mitgliedstaaten durchaus erlaubt, die grundsätzliche Verpflichtung zum Schutz der vertraulichen Kommunikation selbst auszugestalten und mit Ausnahmen zu versehen. Diese Ausnahmen dürften jedoch nicht zur Regel werden.[242] Nach der ständigen Rechtsprechung des EuGH seien die Ausnahmen vom Schutz personenbezogener Daten auf das absolut Notwendige zu beschränken.[243] Außerdem wurden in Anbetracht der Schwere des Eingriffs in die betreffenden Grundrechte besonders hohe Anforderungen an die Rechtfertigung durch eine nationale Regelung gestellt, die die Vorratsdatenspeicherung von Verkehrs- und Standortdaten zu Zwecken der Kriminalitätsbekämpfung vorsieht. Die Vorratsdatenspeicherung könne also allein zur Bekämpfung schwerer Straftaten herangezogen werden.[244] Zu diesem Zweck erlaube die Datenschutzrichtlinie eine gezielte Vorratsspeicherung von Daten, sofern diese hinsichtlich der Art der Daten, der betroffenen Kommunikationsmittel sowie der betroffenen Personen und der Dauer der Speicherung auf das absolut Notwendige beschränkt sei. Immerhin wurde festgestellt, dass eine ausnahmslose, alle Kommunikationsteilnehmer erfassende Vorratsdatenspeicherung, ohne dass jene Personen einen Anlass dazu gegeben hätten, mit Europarecht nicht vereinbar ist.

Im Anschluss daran hat der EuGH im Jahr 2020 zwei neue Urteile gesprochen.[245] Er hat hier zwar im Prinzip die im Jahr 2016 aufgestellten

240 EuGH, C-203/15, C-698/15, 21.12.2016.

241 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. Nr. L 201 vom 31. Juli 2002.

242 EuGH, C-203/15, C-698/15, 21.12.2016, Rn. 88 und 89.

243 EuGH, C-203/15, C-698/15, 21.12.2016, Rn. 96.

244 EuGH, C-203/15, C-698/15, 21.12.2016, Rn. 102 und 103.

245 EuGH, C-623/17, 6.10.2020 sowie EuGH, C-511/18, C-512/18 und C-520/18, 6.10.2020.

strengen Vorgaben an die Rechtmäßigkeit der Vorratsdatenspeicherung aufrechterhalten, jedoch Ausnahmen vom Verbot der Vorratsdatenspeicherung geschaffen. Die möglichen Ausnahmen wurden in einem Katalog in Ansatz gebracht und konkretisiert:

- Im Falle der gegenwärtigen oder vorhersehbaren ernsthaften Bedrohung der nationalen Sicherheit oder zur Bekämpfung schwerer Straftaten dürfen die Mitgliedstaaten per Gesetz die allgemeine und unterschiedslose Aufbewahrung von Verkehrs- und Standortdaten für einen auf das unbedingt erforderliche Maß beschränkten Zeitraum vorsehen. Dieser Zeitraum kann bei fortbestehender Bedrohung verlängert werden.
- Ein Gericht oder eine unabhängige Verwaltungsbehörde muss diese Maßnahmen jeweils überprüfen.
- Auch sei eine gezielte, zeitlich auf das unbedingt Notwendige beschränkte Speicherung von Verkehrs- und Standortdaten erlaubt, die auf der Grundlage objektiver und nicht diskriminierender Faktoren nach Maßgabe der betroffenen Personengruppen oder anhand eines geografischen Kriteriums begrenzt ist.
- Ebenso steht es den Mitgliedstaaten offen, eine allgemeine und unterschiedslose, wenn auch auf das unbedingt notwendige Maß beschränkte Vorratsspeicherung von IP-Adressen oder sogar eine allgemeine und unterschiedslose Vorratsspeicherung nur von Daten vorzunehmen, die sich auf die Identität der Telekommunikationsnutzer beziehen – hier sogar ohne Fristbindung.
- Schließlich hält der EuGH auch Regelungen zur Echtzeiterhebung von unter anderem Verkehrs- und Standortdaten für unionsrechtskonform, sofern diese Erhebung auf Personen beschränkt ist, bezüglich derer der begründete Verdacht besteht, dass sie in der einen oder anderen Weise an terroristischen Aktivitäten beteiligt sind, und wenn diese Datenerhebung einer vorherigen Überprüfung durch ein Gericht oder eine unabhängige Verwaltungsbehörde unterliegt. In dringenden Fällen hat die Überprüfung unverzüglich zu erfolgen.

b) Das deutsche Umsetzungsgesetz

Die Vorratsdatenspeicherungsrichtlinie wurde in Deutschland mit dem Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen vom 21. Dezember 2007 umgesetzt. Dies führte zu Änderungen des TKG, der StPO, des BKAG und

des JVEG. Der neu eingeführte § 113a TKG a. F.[246] verpflichtete die Anbieter öffentlich zugänglicher Telekommunikationsdienste (Abs. 1 Satz 1) dazu, Verkehrsdaten sechs Monate lang zu speichern, damit Auskunftsersuche der berechtigten Stellen unverzüglich beantwortet werden können (Abs. 9). Die Absätze 2 bis 4 sahen eine Vorratsdatenspeicherungspflicht der Anbieter von öffentlich zugänglichen Telefondiensten, Diensten elektronischer Post und Internetzugangsdiensten mit jeweils zu speichernden Datenkategorien vor. Inhaltsdaten waren dabei gemäß Abs. 8 von der Speicherverpflichtung ausgenommen. Zudem wurden gemäß § 113a Abs. 7 TKG die Betreiber von Mobilfunknetzen dazu verpflichtet, Daten über die geografischen Lagen der die jeweilige Funkzelle versorgenden Funkantennen sowie ihre Hauptstrahlrichtung vorzuhalten. Betreffend die Qualität und den Schutz der gespeicherten Daten verlangte Abs. 10, die im Bereich der Telekommunikation erforderliche Sorgfaltspflicht zu beachten. Die im Rahmen der Vorratsdatenspeicherung gespeicherten Daten waren innerhalb eines Monats nach Ablauf der Frist zu löschen (Abs. 11).

Der § 113b TKG a. F. bestimmte die Zwecke, für die die nach § 113a gespeicherten Daten verwendet werden dürfen: zur Verfolgung von Straftaten, zur Abwehr von erheblichen Gefahren für die öffentliche Sicherheit oder zur Erfüllung der gesetzlichen Aufgaben der Verfassungsschutzbehörden des Bundes und der Länder, des Bundesnachrichtendienstes und des Militärischen Abschirmdienstes. Darüber hinaus enthielt der Artikel die Verlangens- und Übermittlungsvoraussetzungen der Daten.

Die Ermächtigungsgrundlage zur Verwendung der Daten im Rahmen der Strafverfolgung wurde mit § 100g StPO a. F. geschaffen. Es handelt sich um eine Erhebungsberechtigung der Daten. Dabei wurden die Voraussetzungen eines Zugriffs auf die Daten geregelt. Die Berechtigung lag vor, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer entweder 1. eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 StPO bezeichnete Straftat oder 2. eine Straftat mittels Telekommunikation begangen hat und der Zugriff für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes erforderlich ist. Außerdem ermächtigt § 20m BKAG dazu, auf die gemäß § 113a TKG a. F. gespeicherten Daten zuzugreifen.

246 Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, vom 21. Dezember 2007 BGBl. I S. 3198 (Nr. 70); Geltung ab dem 01. Januar 2008.

Die Umsetzung der Richtlinie in nationales Recht der EU-Mitgliedstaaten brachte in Ländern, die mit fortgeschrittenen nationalen Standards für den Schutz der Privatsphäre ausgestattet waren, eine Reihe verfassungsrechtlicher Herausforderungen mit sich. Die verfassungsrechtlichen Bedenken gegen das Umsetzungsgesetz wurden in der Literatur vor sowie nach der Einführung der Vorratsdatenspeicherung immer wieder hervorgehoben. In Übereinstimmung mit diesen Bedenken wurden zahlreiche Verfassungsbeschwerden eingereicht.[247] Denn der Bundesverfassungsgerichtshof entschied stets, dass das Recht auf informationelle Selbstbestimmung ein Grundrecht darstelle, das nach dem deutschen Grundgesetz geschützt sei.[248] Das Bundesverfassungsgericht beschloss im März 2010, also erst zwei Jahre nach der Einführung der Vorratsdatenspeicherung, über vielzählige Verfassungsbeschwerden. Nach seinem Urteil stellen die Vorschriften zur Vorratsdatenspeicherung einen Eingriff in das Grundrecht aus Art. 10 Abs. 1 GG dar. Dieser gewährleistet das Fernmeldegeheimnis, das die unkörperliche Übermittlung von Informationen an individuelle Empfänger mit Hilfe des Telekommunikationsverkehrs vor einer Kenntnisnahme durch die öffentliche Gewalt schützt. Folglich liege in der an die Telekommunikationsunternehmen gerichteten Anordnung, Telekommunikationsdaten zu erheben, zu speichern und an eine staatliche Stelle zu übermitteln, jeweils ein Eingriff in Art. 10 Abs. 1 GG vor.[249]

Die Vorratsdatenspeicherung sei zwar nicht schlechthin mit dem Grundgesetz unvereinbar[250] und auch nicht von vornherein unverhältnismäßig im engeren Sinne,[251] jedoch entsprächen die Regelungen zur Datensicherheit, zu den Zwecken und zur Transparenz der Datenverwendung sowie zum Rechtsschutz nicht den verfassungsrechtlichen Anforderungen.[252] Angesichts des Umfangs und der potenziellen Aussagekraft der mit einer solchen Speicherung geschaffenen Datenbestände bedürfe es der gesetzlichen Gewährleistung besonders hoher Standards der Datensicherheit, also eng eingeschränkter sowie konkreter gesetzlicher Regelungen über die Voraussetzungen für die Datenverwendung und deren Umfang

247 Insgesamt legten 34.443 Bürger Verfassungsbeschwerde ein, vgl. *Krempl*, 34.443 Klageschriften gegen die Vorratsdatenspeicherung, heise online v. 29. Februar 2008, abrufbar unter: http://www.heise.de/-185285.html.

248 Siehe zum Beispiel BVerfGE 1, 6 (Mikrozensusurteil); BVerfGE 65, 1 (Volkszählungsurteil).

249 BVerfGE 125, 260 (309 ff.).

250 BVerfGE 125, 260 (316).

251 BVerfGE 125, 260 (318).

252 BVerfGE 125, 260 (347).

sowie hinreichender Vorkehrungen, die der Gesetzgeber zur Transparenz der Datenverwendung sowie zur Gewährleistung eines effektiven Rechtsschutzes und effektiver Sanktionen trifft.

Das Bundesverfassungsgericht erklärte somit die Regelungen zur Vorratsdatenspeicherung für verfassungswidrig und insoweit für nichtig. Der Gerichtshof hat also ausdrücklich auf eine Entscheidung gegen die Gültigkeit der Richtlinie über die Vorratsdatenspeicherung verzichtet und lediglich die innerstaatliche Gesetzgebung dazu aufgefordert, nationale Bestimmungen einzuführen, die die organisatorischen und technischen Schutzvorkehrungen für die Privatsphäre und für personenbezogene Daten in bestimmten Bereichen erhöhen.

c) Erneute Verabschiedung 2015

Nach der Entscheidung des Bundesverfassungsgerichts erklärten die deutsche Regierung und die Fraktionen der CDU/CSU und der SPD am Anfang des Jahres 2015 die Erforderlichkeit der Wiedereinführung der Vorratsdatenspeicherung. Daran anschließend legten beide Fraktionen dem Bundestag einen „Entwurf eines Gesetzes zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten“[253] vor. Obwohl Deutschland wegen der Entscheidung des EuGH nicht zur Umsetzung der Vorratsdatenspeicherungsrichtlinie verpflichtet ist, stimmte der Bundestag im Oktober 2015 für den Gesetzesentwurf der Bundesregierung zur Einführung einer Speicherpflicht und einer Höchstspeicherfrist für Verkehrsdaten, der am 16. Oktober 2015 vom Bundestag ohne wesentliche Änderungen beschlossen wurde. Am 6. November 2015 stimmte der Bundesrat dem Gesetz zu, am 10. Dezember 2015 wurde es vom Bundespräsidenten unterzeichnet und am 17. Dezember 2015 im Bundesgesetzblatt veröffentlicht. Damit wurde die Vorratsdatenspeicherung in Deutschland wiedereingeführt. Mit diesem Gesetz wurden einige Vorschriften vornehmlich in TKG und der StPO geändert und einige Vorgaben in das TKG und die StPO neu eingefügt.

Die wichtigste Änderung beim Gesetz zur Wiedereinführung der Vorratsdatenspeicherung besteht darin, dass der Gesetzgeber gemäß den Anforderungen des Bundesverfassungsgerichts hinsichtlich der Datensicherheit, des Zwecks sowie der Transparenz der Datenverwendung und des Rechtsschutzes die entsprechenden Regelungen zusammengestellt hat. Da-

253 BT-Drs. 18/5088; BT-Drs. 18/5171.

für wurden nicht nur die Straftaten, die die Datenerhebung ermöglichen, konkret ausgestaltet, sondern in §§ 113c bis 113g TKG auch die Vorkehrungen zur Datensicherheit und zur Transparenz der Datenverwendung getroffen. Im Detail wurden Regelungen zur Datenübermittlung nach § 113c TKG, zur Gewährleistung der Datensicherheit nach § 113d TKG, zur Verpflichtung der Protokollierung nach § 113e TKG, über den Anforderungskatalog zur Datensicherheit und Datenqualität nach § 113f TKG sowie zum Sicherheitskonzept nach § 113g TKG mit der Neuregelung des Gesetzes zur Vorratsdatenspeicherung geschaffen.

In der Literatur wurden gegen die Rechtmäßigkeit dieser neuen Regelungen vor allem in Bezug auf die Vereinbarkeit des § 113b TKG mit dem Unionsrecht allerdings schon früh Bedenken angemeldet.[254] Außerdem wurden gegen die wiedereingeführte Vorratsdatenspeicherung[255] wiederum mehrere Verfassungsbeschwerden eingereicht, die erste bereits am 18. Dezember 2015, also nur wenige Tage nach der Verabschiedung des neuen Vorratsdatenspeicherungsgesetzes.[256] Seitdem wurden kontinuierlich weitere Verfassungsbeschwerden gegen das Gesetz eingelegt.[257] Darüber hinaus wurde vom Internetverband Eco zusammen mit dem Münchener Internetprovider SpaceNet AG eine Klage vor dem Verwaltungsgericht Köln eingereicht. Die Klage richtete sich an das Verwaltungsgericht, weil vor dem Verwaltungsgericht, anders als bei Verfassungsbeschwerden, bei denen ein beschränkter Prüfungsrahmen angelegt würde, das gesamte

254 *Roßnagel*, Die neue Vorratsdatenspeicherung – der nächste Schritt im Ringen um Sicherheit und Grundrechtsschutz, NJW 2016, 533, 538; *Derksen*, Unionsrechtskonforme Spielräume für anlasslose Speicherung von Verkehrsdaten?, NVwZ 2017, 1005.

255 Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten, Bundesgesetzblatt Jahrgang 2015 Teil I Nr. 51, ausgegeben zu Bonn am 17. Dezember 2015.

256 1 BvR 3156/15.

257 1 BvR 17/16: Das Gesetz wurde hier deswegen kritisiert, weil die „anlasslos vorsorgliche Speicherung von Telekommunikationsdaten aller Bürger auf Grund ihrer Streuweite und Intensität einen ganz erheblichen Eingriff in das Fernmeldegeheimnis und den Schutz der Persönlichkeit bedeute."; 1 BvR 141/16; 1 BvR 229/16: Es wurde behauptet, dass die anlasslose Datenspeicherung bei den schrecklichen Anschlägen in Frankreich wirkungslos war; 1 BvR 2683/16: Hier wurde inhaltlich insbesondere der Punkt der Überwachungsgesamtrechnung aufgegriffen; 1 BvR 2840/16: Die Beschwerde führt den Punkt der Überwachungsgesamtrechnung weiter und warnt vor Gefahren, dass moderne Kommunikationsmittel wie Handys aufgrund der Vorratsdatenspeicherung zu elektronischen Fußfesseln würden. Die Beschwerde wurde ohne Begründung abgelehnt.

maßgebliche Recht berücksichtigt werden kann, also auch die seit 2016 geltende Rechtsprechung des EuGH.[258] Dabei wurde zugleich ein Eilantrag gestellt, der allerdings zunächst mit Beschluss vom 25. Januar 2017 abgelehnt wurde.[259] Gegen den Beschluss wurde nachfolgend erfolgreich Beschwerde vor dem Oberverwaltungsgericht für das Land Nordrhein-Westfalen eingelegt.[260] Das Oberverwaltungsgericht bestätigte damit die Unvereinbarkeit der deutschen Gesetzgebung mit dem Unionsrecht, speziell mit dem Art. 15 Abs. 1 der Richtlinie 2002/58[261] und die Verletzung der durch Art. 16 der Charta der Grundrechte der Europäischen Union geschützten unternehmerischen Freiheit der Antragstellerin.[262] Mit dem Beschluss wurde dem Eilantrag stattgegeben. Eine abschließende Klärung der grundlegenden verfassungsrechtlichen und unionsrechtlichen Fragestellungen sei allein in einem Hauptsacheverfahren möglich.[263] In der Folge setzte die Bundesnetzagentur die Pflicht zur Vorratsdatenspeicherung bis zur Entscheidung einer Klage im Hauptsacheverfahren aus.[264] Das Verwaltungsgericht Köln stellte danach in seiner Entscheidung fest, dass der nach § 113a TKG Verpflichtete gemäß § 113b TKG gerade nicht dazu verpflichtet ist, solche Daten gemäß § 113a TKG zu speichern. Die Entscheidung wurde damit begründet, dass die genannte Pflicht nicht mit Europarecht, speziell dem Art. 15 Abs. 1 der Richtlinie 2002/58, vereinbar sei. Da der EuGH feststellte, dass eine ausnahmslose, alle Kommunikationsteilnehmer erfassende Vorratsdatenspeicherung, ohne dass jene Personen einen Anlass dazu gegeben hätten, nicht mit Europarecht vereinbar sei,

258 SpaceNet und eco klagen gegen Vorratsdatenspeicherung. In: Süddeutsche Zeitung, 9. Mai 2017, abgerufen am 2. Februar 2019.
259 VG Köln, 9 L 1009/16, Beschluss am 25. Januar 2017.
260 OVG NRW, 13 B 238/17, Beschluss am 22. Juni 2017.
261 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation – Datenschutzrichtlinie für elektronische Kommunikation – (ABl. L 201, S. 37), zuletzt geändert durch die Richtlinie 2009/136/EG des Europäischen Parlaments und Rates vom 25. November 2009 (ABl. L 337, S. 11) im Lichte der Grundrechte aus Art. 7, 8 und 11 sowie Artikel 52 Abs. 1 der Charta der Grundrechte der Europäischen Union. Vgl. EuGH, Urteil vom 21. Dezember 2016 – C-203/15 und C-698/15 – Tele2 Sverige AB und Watson.
262 OVG NRW, 13 B 238/17, Rn. 33.
263 OVG NRW, 13 B 238/17, Rn. 88.
264 *Holland*, Bundesnetzagentur setzt Vorratsdatenspeicherung aus, heise online v. 28. Juni 2017, abrufbar unter: https://www.heise.de/-3757527.html.

regelte das deutsche Gesetz in §§ 113a und 113b TKG dies nach Ansicht des VG Köln rechtswidrig.[265]

Rein formell gesehen war die Vorratsdatenspeicherung damit nicht abgeschafft, sondern lediglich ihre Umsetzung bis zur Schaffung der notwendigen Rechtssicherheit aufgeschoben.[266] Die Entscheidungen des Bundesverfassungsgerichts über die aktuellen Gesetze zur Vorratsdatenspeicherung bleiben abzuwarten. Das Gericht stellte die grundsätzliche Rechtmäßigkeit der Vorratsdatenspeicherung fest, bemängelte jedoch das Datenschutzniveau der Vorratsdatenspeicherungsgesetze a. F. und erklärte das Gesetz daher für nichtig. Das Bundesverfassungsgericht stellte in seiner Entscheidung zum Datenschutz fest, dass die Rechtmäßigkeit deutscher Gesetze, die nicht auf eine EU-Richtlinie zurückzuführen und nicht durch Unionsrecht determiniert sind, grundsätzlich nicht an Unionsrecht zu messen ist, und dass eine Vorlage an den EuGH damit grundsätzlich ausscheidet.[267] Das Gericht hat in seinem Beschluss vom 8. Juni 2016 eine Aussetzung des Vollzugs der §§ 113a und 113b TKG abgelehnt, da der in der bloßen Speicherung der Verkehrsdaten liegende Nachteil für Freiheit und Privatheit der Einzelnen erst durch einen Abruf der Daten zu einer irreparablen Grundrechtsbeeinträchtigung führen könne.[268] Auch sei eine Aussetzung des Vollzugs von §§ 100g, 101a und 101b StPO mit der Begründung nicht geboten, dass der Gesetzgeber mit § 100g Abs. 2 StPO den Abruf von Verkehrsdaten i. S. d. § 113b TKG von qualifizierten Voraussetzungen abhängig gemacht habe. Diese lassen das Gewicht der durch den Vollzug der Vorschrift drohenden Nachteile für die Übergangszeit bis zur Entscheidung über die Hauptsache hinnehmbar und im Vergleich mit den Nachteilen für das öffentliche Interesse an einer effektiven Strafverfolgung weniger gewichtig erscheinen.[269] Bis zur eventuellen Ungültigkeitserklärung des Bundesverfassungsgerichts bleiben die aktuellen Gesetze zur Vorratsdatenspeicherung jedenfalls gültig. Es ist folglich bedeutsam, den aktuellen rechtlichen Inhalt eingehend zu betrachten, damit man die Konstruktion der Gesetze und deren Datenschutzniveau einsehen und die eventuellen Bedenken einschätzen kann.

---

265 VG Köln, 9 K 7417/17, Rn. 87.

266 *Levenshtein*, Vorratsdatenspeicherung auf Eis gelegt, industr.com v. 29. Juni 2017, abrufbar unter https://www.industr.com/-2296251.

267 BVerfGE 125, 260 (306 f.).

268 BVerfG, 08.06.2016, 1 BvQ 42/15, NVwZ 2016, 1240, Rn. 26.

269 BVerfG, 08.06.2016, 1 BvQ 42/15, NVwZ 2016, 1240, Rn. 20 und 22.

2. Aktuelle Rechtslage

Vom Schutz des Fernmeldegeheimnisses sind nicht nur die Kommunikationsinhalte, sondern auch die näheren Umstände der Telekommunikation erfasst. Das Recht auf Fernmeldegeheimnis verhindert, dass der Meinungs- und Informationsaustausch mittels Telekommunikationsanlagen deswegen unterbleibt oder nach Form und Inhalt verändert verläuft, weil die Beteiligten mit Überwachung rechnen müssen.[270] § 100g StPO enthält dabei Eingriffsermächtigungen zugunsten der Strafverfolgungsbehörden. Das Gesetz zur Einführung einer Speicherpflicht und einer Höchstspeicherpflicht für Verkehrsdaten vom 10. Dezember 2015[271] bildet den rechtlichen Rahmen der neuen Vorratsdatenspeicherung. Es handelt sich dabei um ein „Doppeltürmodell",[272] das die konkreten Verantwortlichkeiten und Voraussetzungen mit einem Zweischritt in zwei verschiedene Gesetze aufspaltet: auf der einen Seite steht die Aufnahme eines Gesetzes über die Erhebung, Speicherung und Übermittlung ins TKG (Speicherpflicht und Bestimmung der Verantwortlichen, Art der zu speichernden Daten, Speicherdauer und Übermittlungsberechtigung) sowie auf der anderen Seite die Aufnahme eines Gesetzes über die Datenerhebung in die StPO (Zugriffsvoraussetzungen für den Abruf durch die Strafverfolgungsbehörden). Hiermit wurden die §§ 113a–g TKG neu eingeführt und der § 100g StPO geändert. Im Folgenden soll die aktuelle Rechtslage unter der neu eingeführten Vorratsdatenspeicherung untersucht werden. Um den Sinn der Einführung der Vorratsdatenspeicherung richtig zu erfassen, ist es zunächst notwendig, die Definition der Begriffe „Bestandsdaten" und „Verkehrsdaten" zu verdeutlichen. Des Weiteren ist zu erklären, welche Daten vor der Einführung der Vorratsdatenspeicherung gespeichert und unter welchen Voraussetzungen diese zu Ermittlungszwecken verwendet werden durften. Anschließend sollen die Vorschriften zur Vorratsdatenspeicherung vorgestellt, die Änderungen nach der Einführung der Vorratsdatenspeicherung konkret analysiert und die Datenspeicherung und -verwendung vor und nach der Neueinführung der Vorratsdatenspeicherung miteinander verglichen werden.

Die Rechtsgrundlagen der Speicherung, Verarbeitung und Nutzung personenbezogener Daten durch die Telekommunikationsdiensteanbieter sollen wie folgt skizziert werden: Nach dem Bundesdatenschutzgesetz

270 BVerfGE 100, 313 (359).
271 BGBl. I 2015, S. 2218, in Kraft seit dem 18. Dezember 2015.
272 *Dalby*, Vorratsdatenspeicherung – Endlich?!, KriPoZ 2016, 113, 113.

(BDSG), das bezweckt, den Einzelnen vor einer Beeinträchtigung in seinem Persönlichkeitsrecht durch den Umgang mit seinen personenbezogenen Daten zu schützen, sind die Erhebung, Verarbeitung und Nutzung personenbezogener Daten grundsätzlich verboten. Sie sind nur auf Basis eines Erlaubnistatbestandes – auf Grundlage eines Erlaubnistatbestandes im BDSG, einer anderen Rechtsvorschrift oder einer Einwilligung des Betroffenen – zulässig.[273] Das BDSG fordert außerdem Datenvermeidung und -sparsamkeit.[274] Die Grundidee ist, dass bei der Datenverarbeitung nur so viele personenbezogene Daten gesammelt werden, wie für die jeweilige Anwendung unbedingt notwendig sind.[275]

Auf dieser Rechtsgrundlage sind §§ 95–98 TKG für die Datenerhebung und -verwendung von Telekommunikationsunternehmen einschlägig; ihre Ausnahmen bilden §§ 111–113 TKG. Daten, die nach dem TKG durch die Telekommunikationsdiensteanbieter gespeichert und verwendet werden können, lassen sich in Bestandsdaten und Verkehrsdaten (auch als Verbindungsdaten bezeichnet) unterteilen. Bestandsdaten sind nach § 3 Nr. 3 TKG Daten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden, während es sich nach § 3 Nr. 30 TKG um Verkehrsdaten handelt, wenn Daten bei der Erbringung eines Telekommunikationsdienstes erhoben, verarbeitet oder genutzt werden. Standortdaten bilden einen Unterfall von Verkehrsdaten.

Bestandsdaten dürfen ursprünglich nach § 95 TKG nur erhoben und verwendet werden, soweit dies zur Vertragserfüllung erforderlich ist. Die Erhebung und die Verwendung von Bestandsdaten dürfen also nicht erlaubt werden, wenn dies nicht für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses erforderlich ist. § 111 TKG bildet jedoch eine bedeutende Ausnahme, nach der Anbie-

273 § 4 BDSG.

274 § 3a BDSG: „Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten und die Auswahl und Gestaltung von Datenverarbeitungssystemen sind an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen. Insbesondere sind personenbezogene Daten zu anonymisieren oder zu pseudonymisieren, soweit dies nach dem Verwendungszweck möglich ist und keinen im Verhältnis zu dem angestrebten Schutzzweck unverhältnismäßigen Aufwand erfordert."

275 Das Konzept wurde gesetzlich erstmals in § 3 Abs. 4 TDDSG im Juli 1997 normiert: „Die Gestaltung und Auswahl technischer Einrichtungen für Teledienste hat sich an dem Ziel auszurichten, keine oder so wenige personenbezogene Daten wie möglich zu erheben, zu verarbeiten und zu nutzen."

ter, die geschäftsmäßig Telekommunikationsdienste erbringen oder daran mitwirken und dabei Rufnummern oder andere Anschlusskennungen vergeben, für die Auskunftsverfahren nach §§ 112 und 113 TKG bestimmte Informationen zu erheben und unverzüglich zu speichern haben.[276] Es handelt sich dabei um eine Speicherpflicht der Anbieter von Telefondiensten, Mobilfunktelefonen und Diensten elektronischer Postfächer.[277] Nach § 111 TKG sind die folgenden Bestandsdaten auch dann zu erheben und zu speichern, wenn sie für betriebliche Zwecke nicht erforderlich sind:

1. Rufnummer (stattdessen die Kennungen der elektronischen Postfächer bei Diensten des elektronischen Postfaches),
2. Name und Anschrift des Anschlussinhabers (statt des Anschlussinhabers des Inhabers des elektronischen Postfachs bei elektronischen Postfachdiensten),
3. das Geburtsdatum,
4. die Anschrift des Anschlusses bei Festnetzanschlüssen bzw. die Gerätenummer des überlassenen Mobilfunktelefons,
5. das Datum des Vertragsbeginns sowie
6. die bisher noch nicht erhobenen Daten, sofern dem Anbieter eine Erhebung der Daten ohne besonderen Aufwand möglich ist.

Auf gespeicherte Bestandsdaten darf im automatisierten Verfahren nach §§ 111, 112 TKG (dann nur auf die in § 111 Abs. 1 TKG genannten Daten) oder im Rahmen eines manuellen Auskunftsverfahrens nach § 113 TKG zugegriffen werden. §§ 112, 113 TKG bestimmen jeweils das automatisierte oder manuelle Auskunftsverfahren einschließlich der ersuchenden Stellen und der Ersuchungsformen. Dabei ist nach § 113 Abs. 5 TKG dafür Sorge

276 Vgl. *Albrecht, H.-J.*, Schutzlücken durch Wegfall der Vorratsdatenspeicherung – Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten: Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht, im Auftrag des Bundesministerium der Justiz, S. 21: „Der Begriff der ‚kleinen Vorratsdatenspeicherung' bietet sich an, da auch hier Daten auf Vorrat gespeichert werden, die für die eigentlichen Zwecke der Anbieter nicht erforderlich sind, die aber die Verfolgung von Ordnungswidrigkeiten nach dem TKG oder dem UWG ermöglichen sollen oder die für die Erledigung der Auskunftsersuchen der in § 112 Abs. 2 TKG genannten Stellen benötigt werden."

277 An den Daten, die bei elektronischen Postfachdiensten zu speichern sind, wird Kritik geübt, dass es sich um Telemedienbestandsdaten handele, so dass die Vorschrift grundsätzlich im falschen Gesetz enthalten und zudem durch die Verweisungstechnik auch nicht besonders normenklar sei; vgl. *Brunst*, Anonymität im Internet, S. 396 m. w. N.

zu tragen, dass jedes Auskunftsverlangen durch eine verantwortliche Fachkraft auf Einhaltung der in § 113 Abs. 2 TKG genannten formalen Voraussetzungen geprüft und die weitere Bearbeitung des Verlangens erst nach einem positiven Prüfergebnis freigegeben wird. Eine Strafverfolgungsbehörde darf nach § 100j Abs. 1 Satz 1 StPO Auskunft über die nach den §§ 95 und 111 TKG erhobenen Daten verlangen. Die Zugriffsregelung in der StPO (§ 100j StPO) wird zu einer Übermittlungspflicht für Telekommunikationsdiensteanbieter (§ 113 Abs. 4 TKG) konkretisiert. Wird Auskunft über Daten, mittels derer der Zugriff auf Endgeräte oder auf Speichereinrichtungen, die in diesen Endgeräten oder hiervon räumlich getrennt eingesetzt werden, geschützt wird, verlangt, darf dies nach § 100j Abs. 3 Satz 1 StPO nur auf Antrag der Staatsanwaltschaft durch das Gericht angeordnet werden. Es besteht bei Gefahr im Verzug die Möglichkeit, die Anordnung auch durch die Staatsanwaltschaft oder ihre Ermittlungspersonen mit einer Nachholung der gerichtlichen Entscheidung zu treffen (§ 100j Abs. 3 Satz 2 und 3 StPO). Über die Auskunftserteilung ist die betroffene Person mit Ausnahme des Vorliegens einer Unterbleibens- oder Zurückstellungsvoraussetzung der Benachrichtigung zu benachrichtigen (§ 100j Abs. 4 StPO).

§ 96 TKG bildet einen Erlaubnistatbestand der Erhebung und der Verwendung von Verkehrsdaten. Es setzt die Erforderlichkeit zu den im 2. Abschnitt des TKG genannten oder durch andere gesetzliche Vorschriften begründeten Zwecke oder zum Aufbau weiterer Verbindungen voraus. Nach § 96 TKG dürfen die folgenden Verkehrsdaten erhoben werden:

1. die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung, personenbezogene Berechtigungskennungen, bei Verwendung von Kundenkarten auch die Kartennummer, bei mobilen Anschlüssen auch die Standortdaten,
2. der Beginn und das Ende der jeweiligen Verbindung, die übermittelten Datenmengen, soweit die Entgelte davon abhängen,
3. der vom Nutzer in Anspruch genommene Telekommunikationsdienst,
4. die Endpunkte von festgeschalteten Verbindungen, ihren Beginn und ihr Ende und – soweit Entgelte davon abhängen – die übermittelten Datenmengen sowie
5. sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten.

Nach §§ 96, 97 TKG werden die Verkehrsdaten erhoben und verwendet, um einen technisch korrekten Verbindungsaufbau zu ermöglichen und die notwendigen Grundlagen für eine korrekte Entgeltermittlung und

-abrechnung zu schaffen. Die Abrechnungsdaten dürfen bis sechs Monate nach Versendung der Rechnung gespeichert werden, für die Abrechnung nicht erforderliche Daten hingegen sind unverzüglich zu löschen (§ 97 Abs. 3 TKG). Standortdaten als ein Unterfall von Verkehrsdaten dürfen außerdem nach § 98 TKG nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Umfang und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer dem Anbieter des Dienstes mit Zusatznutzen seine Einwilligung erteilt hat. Auf die Verkehrsdaten darf auf Grundlage des § 100g StPO zugegriffen werden. Vor der Vorratsdatenspeicherung durfte aber auf die nach §§ 96, 97 TKG gespeicherten Verkehrsdaten nur zugegriffen werden, soweit die Daten zum Zeitpunkt eines Auskunftsersuchens noch vorhanden waren.[278] Denn es bestand damals keine Regelung über Datenspeicherungs- und Datenübermittlungspflichten.

Auf dieser Rechtsgrundlage kommt es vor, dass Telekommunikationsdiensteanbieter unabhängig von §§ 96, 97 und 98 TKG nach der Vorratsdatenspeicherung (§§ 113a–g TKG) verpflichtet sind, die darin genannten Verkehrsdaten zu speichern und unter bestimmten Voraussetzungen an eine befugte Stelle zu übermitteln. Im Folgenden soll näher darauf eingegangen werden, wer welche Verkehrsdaten für welche Dauer nach §§ 113a–g TKG i. V. m. § 100g StPO zu speichern hat und unter welchen Voraussetzungen die Strafverfolgungsbehörden zu Ermittlungszwecken auf diese Daten zugreifen dürfen. Dabei soll die Eingriffsintensität der Vorratsdatenspeicherung untersucht und anschließend bewertet werden, ob es Regelungen für flankierende Maßnahmen gibt, die die Eingriffsintensität der Vorratsdatenspeicherung mildern sollen, und ob diese Regelungen hinreichend sind.

a) Zu speichernde Daten

Es sind Erbringer öffentlich zugänglicher Telekommunikationsdienste für Endnutzer, die im Rahmen der Vorratsdatenspeicherung dazu verpflichtet sind, bestimmte Verkehrsdaten für die unverzügliche Beantwortung auf Auskunftsersuchen der berechtigten Stellen zu speichern (§ 113a Abs. 1 Satz 1 TKG). Dies sind Telekommunikationsdiensteunternehmen i. S. d. § 3 Nr. 6 lit. a) TKG, also nicht bloß bei der Übermittlung von Daten

278 § 100g StPO a. F. Gesetz zur Änderung der Strafprozessordnung vom 20. Dezember 2001, BGBl. 2001, I. Nr. 73, S. 3879.

mitwirkende Unternehmen – etwa Anbieter, die ihren Kunden nur eine kurzzeitige Nutzung des Telekommunikationsanschlusses ermöglichen (Hotspots in Hotels, Restaurants und Cafés).[279] Es handelt sich dabei vielmehr um Erbringer öffentlich zugänglicher Telefon- sowie Internetzugangsdienste. Wer öffentlich zugängliche Telekommunikationsdienste für Endnutzer erbringt, aber nicht alle der nach Maßgabe der §§ 113b bis 113g TKG zu speichernden Daten selbst erzeugt oder verarbeitet, hat sicherzustellen, dass die nicht von ihm selbst bei der Erbringung seines Dienstes erzeugten oder verarbeiteten Daten gemäß § 113b TKG von einem anderen gespeichert werden, und er hat der Bundesnetzagentur auf deren Verlangen hin unverzüglich mitzuteilen, wer diese Daten speichert (§ 113a Abs. 1 Satz 2 TKG).

Die jeweils bei den unterschiedlichen Telekommunikationsdiensten zu speichernden Daten regelt § 113b Abs. 2 Satz 1 TKG.

Bei den Erbringern von Telefondiensten sind die folgenden Daten zu speichern:

1. Die Rufnummer oder eine andere Kennung des anrufenden und des angerufenen Anschlusses sowie bei Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses,
2. Datum und Uhrzeit von Beginn und Ende der Verbindung,
3. Angaben zu dem genutzten Dienst,
4. bei mobilen Telefondiensten die internationale Kennung mobiler Teilnehmer für den anrufenden und den angerufenen Anschluss (IMSI), die internationale Kennung des anrufenden und des angerufenen Endgerätes (IMEI) sowie Datum und Uhrzeit der ersten Aktivierung des Dienstes, wenn Dienste im Voraus bezahlt wurden,
5. bei Internet-Telefondiensten auch die IP-Adressen des anrufenden und des angerufenen Anschlusses und zugewiesene Benutzerkennungen.

Satz 1 gilt entsprechend bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht und für unbeantwortete oder wegen eines Eingriffs des Netzwerkmanagements erfolglose Anrufe. Das heißt, die Speicherpflicht wird mit § 113b Abs. 2 Satz 2 Nr. 2 TKG auf nicht entgegengenommene oder erfolglose Anrufe ausgedehnt. Bei der Übermittlung einer Nachricht sind anstelle der Angaben nach Satz 1 Nr. 2 die Zeitpunkte der Versendung und des Empfangs der Nachricht zu speichern.

279 Erbringer zeichnen sich dadurch aus, dass den Kunden regelmäßig ein eigener, in der Regel auf unbestimmte Dauer angelegter Telekommunikationsanschluss zur selbständigen Verwendung überlassen wird, vgl. BT-Drs. 18/5088, S. 37.

Als eine bemerkenswerte Regelung muss § 113b Abs. 3 Nr. 1 TKG bezeichnet werden, der insbesondere die Pflicht zur Speicherung der dynamischen IP-Adresse für Erbringer öffentlich zugänglicher Internetzugänge regelt. Dynamische IP-Adressen, die sowohl nach Einschätzung des EuGH als auch nach der des BGH als personenbezogene Daten gelten und folglich besonders zu schützen sind,[280] müssen von den Telekommunikationsanbietern im Sinne der Vorratsdatenspeicherung gespeichert werden. Für Bestandsdatenauskünfte zu dynamischen IP-Adressen darf auf nach § 113b TKG gespeicherte Verkehrsdaten zurückgegriffen werden. Die Speicherung der dynamischen IP-Adresse eröffnet neue Möglichkeiten für die Verfolgungsbehörden im Rahmen der Ermittlung von Straftätern.[281] Bei den Erbringern von Internetzugangsdiensten sind die folgenden Daten zu speichern:

1. Die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse,
2. eine eindeutige Kennung des Anschlusses, über den die Internetnutzung erfolgt, sowie eine zugewiesene Benutzerkennung sowie
3. Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse.

Laut Gesetzgeber sollen die „eindeutige Kennung des Anschlusses" sowie die „zugewiesene Benutzerkennung" der Praxis die Rückverfolgung und Identifizierung der Quelle eines Kommunikationsvorgangs besser ermöglichen.[282] Die Gesetzesbegründung schweigt sich jedoch darüber aus, was diese Begrifflichkeiten bedeuten, die neben der dynamischen IP-Adresse beiordnend geregelt sind.

Im Fall der Nutzung mobiler Telefondienste oder der mobilen Nutzung von öffentlich zugänglichen Internetzugangsdiensten sind darüber hinaus zusätzlich auch Standortdaten bei Beginn aller Mobiltelefonate sowie einer

---

280 EuGH, C-582/14, 19.10.2016; BGH, VI ZR 135/13, 16.05.2017.

281 Trotz enormer praktischer Wichtigkeit dynamischer IP-Adressen im Zusammenhang mit Cybercrime (vgl. den Abschlussbericht BKA 2011 – Stand der statistischen Datenerhebung im BKA zu den Auswirkungen des Urteils des Bundesverfassungsgerichts zu „Mindestspeicherfristen", S. 5) wehrten sich Dienstunternehmen teilweise auch explizit gegen die Abfrage der dynamischen IP-Adresse. Dies geschah unter Verweis auf die ungeklärte Rechtsgrundlage (vgl. *Dalby*, Vorratsdatenspeicherung – Endlich?!, KriPoZ, 2016, 113, 116 m. w. N.), weil das Dienstunternehmen die IP-Adressen nicht für Abrechnungszwecke bei der heutigen Verbreitung von Flatrate-Tarifen benötigt.

282 BT-Drs. 18/5088, S. 39.

mobilen Internetnutzung, also die konkreten Bezeichnungen der Funkzellen, zu speichern.

Der Kommunikationsinhalt, Daten über aufgerufene Internetseiten und Daten von Diensten der elektronischen Post dürfen nicht gespeichert werden (§ 113b Abs. 5 TKG). Wird auch der Inhalt bei einer Kurz-, Multimedia- oder ähnlichen Nachricht gespeichert, muss die ganze Nachricht von Speicherungsgegenständen ausgenommen werden.[283] Die Daten, die nach der Vorratsdatenspeicherung durch die Erbringer öffentlich zugänglicher Telekommunikationsdiente für Endnutzer gespeichert werden müssen, greifen weit über den Speicherumfang vor der Vorratsdatenspeicherung hinaus. Der Telekommunikationsanbieter ist daher dazu verpflichtet, eine zeitlich längere und datenmäßig umfangreichere Speicherung vorhandener Daten vorzunehmen als dies abrechnungstechnisch erforderlich wäre. Dies führt zu einer relativ langen Speicherung einer enormen Menge an Daten getrennt von §§ 95–98 TKG.[284]

Tabelle 1: Synopse der grundsätzlich abfragbaren Datenarten gem. §§ 96 und 113a TKG[285]

§ 96 TKG	**§ 113b TKG**
Abs. 1 Satz 1 Nr. 1: die Nummer oder Kennung der beteiligten Anschlüsse oder der Endeinrichtung personenbezogene Berechtigungskennungen die Kartennummer bei Verwendung von Kundenkarten	Abs. 2 Satz 1 Nr. 1: – die Rufnummer oder eine andere Kennung des anrufenden und des angerufenen Anschlusses sowie bei Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses Abs. 2 Satz 1 Nr. 4: bei mobilen Telefondiensten – die internationale Kennung mobiler Teilnehmer für den anrufenden und den angerufenen Anschluss

283 *Roßnagel*, Die neue Vorratsdatenspeicherung – der nächste Schritt im Ringen um Sicherheit und Grundrechtsschutz, NJW 2016, 533, 535.

284 Zum Vergleich der gemäß § 96 TKG zu speichernden Daten mit den gemäß § 113a TKG zu speichernden Daten siehe Tabelle 1.

285 Vgl. *Albrecht, H.-J.*, Schutzlücken durch Wegfall der Vorratsdatenspeicherung – Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten: Gutachten des Max-

	– die internationale Kennung des anrufenden und des angerufenen Endgerätes Abs. 2 Satz 1 Nr. 5: im Fall von Internet-Telefondiensten – auch die *Internetprotokoll-Adressen* des anrufenden und des angerufenen Anschlusses – zugewiesene *Benutzerkennungen* Abs. 3 Nr. 1: im Fall von Internetzugangsdiensten – die dem Teilnehmer für eine Internetnutzung zugewiesene *Internetprotokoll-Adresse* Abs. 3 Nr. 2: im Fall von Internetzugangsdiensten – eine *eindeutige Kennung* des Anschlusses, über den die Internetnutzung erfolgt – eine zugewiesene *Benutzerkennung*
Abs. 1 Satz 1 Nr. 2: den Beginn und das Ende der jeweiligen Verbindung nach Datum und Uhrzeit Abs. 1 Satz 1 Nr. 4: die Endpunkte von festgeschalteten Verbindungen und deren Beginn und Ende nach Datum und Uhrzeit	Abs. 2 Satz 1 Nr. 2: – Datum und Uhrzeit von Beginn und Ende der Verbindung Abs. 2 Satz 1 Nr. 4 c): bei im Voraus bezahlter mobiler Telefondienste – Datum und Uhrzeit der ersten Aktivierung des Dienstes Abs. 2 Satz 2 Nr. 2: – *Datum und Uhrzeit von unbeantworteten* oder wegen eines Eingriffs

Planck-Instituts für ausländisches und internationales Strafrecht, im Auftrag des Bundesministeriums der Justiz, S. 29.

	des Netzwerkmanagements *erfolglosen Anrufen* Abs. 3 Nr. 3: im Fall von Internetzugangsdiensten – Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewiesenen Internetprotokoll-Adresse unter Angabe der jeweils geltenden Zeitzone.
Abs. 1 Satz 1 Nr. 3: den vom Nutzer in Anspruch genommenen Telekommunikationsdienst	Abs. 2 Satz 1 Nr. 3: – Angaben zum genutzten Telefondienst, wenn im Rahmen des Telefondienstes unterschiedliche Dienste genutzt werden können
Abs. 1 Satz 1 Nr. 2: soweit die Entgelte davon abhängen, *die übermittelten Datenmengen* Abs. 1 Satz 1 Nr. 4: soweit die Entgelte davon abhängen, *die übermittelten Datenmengen*	
Abs. 1 Satz 1 Nr. 5: sonstige zum Aufbau und zur Aufrechterhaltung der Telekommunikation sowie zur Entgeltabrechnung notwendige Verkehrsdaten	Abs. 2 Satz 2 Nr. 1: bei der Übermittlung einer Kurz-, Multimedia- oder ähnlichen Nachricht *– die Zeitpunkte der Versendung und des Empfangs der Nachricht*
Abs. 1 Satz 1 Nr. 1: bei mobilen Anschlüssen auch die Standortdaten	Abs. 4 Satz 1 und 2: – bei mobilen Telefondiensten die Bezeichnungen der Funkzellen, die durch den anrufenden und den angerufenen Anschluss bei Beginn der Verbindung genutzt werden – im Fall der mobilen Nutzung öffentlich zugänglicher Internetzugangsdienste die Bezeichnung der bei Beginn der Internetverbindung genutzten Funkzelle

§ 113b Abs. 6 TKG bestimmt hingegen auch die Daten, die nach § 113b TKG nicht gespeichert werden dürfen. Nach der Entscheidung des Bundesverfassungsgerichts, der zufolge es verfassungsrechtlich geboten ist, zumindest für einen engen Kreis auf besondere Vertraulichkeit angewiesener Telekommunikationsverbindungen ein grundsätzliches Übermittlungsverbot vorzusehen,[286] sieht § 113b Abs. 6 TKG vor, dass Daten, die den in § 99 Abs. 2 TKG genannten Verbindungen zugrunde liegen, nicht im Sinne der Vorratsdatenspeicherung gespeichert werden dürfen. Demgegenüber sind die Daten derer, die anderen als den oben genannten Verschwiegenheitsverpflichtungen unterliegen, zu speichern. Nach § 100g Abs. 4 StPO ist die Erhebung von Verkehrsdaten nach § 100g Abs. 2 StPO, auch in Verbindung mit Abs. 3 Satz 2, die sich gegen eine der in § 53 Abs. 1 Satz 1 Nr. 1 bis 5 genannten Personen – z. B. Geistliche, Verteidiger des Beschuldigten, Rechtsanwälte – richtet und die voraussichtlich Erkenntnisse erbringen würde, über die diese das Zeugnis verweigern dürfte, unzulässig. Dennoch erlangte Erkenntnisse dürfen nicht verwendet werden.

Das TKG erfordert keinen Anlass zur Speicherung der in § 113b genannten Daten, sondern sieht die vorrätige Speicherung von Verkehrsdaten *aller* Personen vor, um das Vorhandensein der erforderlichen Daten für eventuelle Anfragen sicherzustellen. Konsequenterweise macht § 113b TKG die Speicherung der hier genannten Verkehrsdaten nicht davon abhängig, ob ein Zusammenhang mit schweren Straftaten besteht bzw. ob die Daten geeignet sind, auf irgendeine Weise zur Bekämpfung schwerer Kriminalität beizutragen oder eine schwerwiegende Gefahr für die öffentliche Sicherheit zu verhindern. Eine solche Zweckbeschränkung besteht ausschließlich für die Verwendung der Daten gemäß § 113c TKG. Der Europäische Gerichtshof erteilt einer anlasslosen Speicherung von Daten, ohne dass jene Personen einen Anlass dazu gegeben haben, also eine Absage.[287] Nach der Datenschutzrichtlinie 2002/58 ist eine allgemeine Speicherung von Daten ohne ausreichende begrenzende Kriterien nicht mit Unionsrecht vereinbar.[288] In diesem Zusammenhang hat das OVG Münster im Wege der einstweiligen Anordnung festgestellt, dass der dort klagende Internetzugangsdiensteanbieter bis zum rechtskräftigen Abschluss des Hauptsacheverfahrens nicht dazu verpflichtet ist, die in § 113b Abs. 3 TKG genannten Verkehrsdaten zu speichern, weil diese Pflicht nicht mit

286 BVerfGE 125, 260 (334).
287 EuGH, C-203/15, C-698/15, 21.12.2016, Rn. 105.
288 EuGH, C-203/15, C-698/15, 21.12.2016, Rn. 108.

Unionsrecht vereinbar ist.[289] Trotz der Entscheidung des EuGH werden in Deutschland im Rahmen der Vorratsdatenspeicherung bestimmte Verkehrsdaten aller Personen anlasslos gespeichert. Insoweit baut der deutsche Gesetzgeber nicht darauf auf, dass der EuGH die eine oder andere Variante der Vorratsdatenspeicherung für unzulässig erklärt, sondern dass in der Entscheidung des EuGH die Gründe, die die Richtlinie zur Vorratsdatenspeicherung und eine entsprechende nationalstaatliche Umsetzung grundrechtswidrig machen würden, *in Summe* aufgezählt werden.[290] Der Gesetzgeber hält weiterhin an der Anlasslosigkeit der Speicherung fest, wobei er gleichzeitig verschiedene Forderungen umsetzt: Nicht alle verfügbaren Daten werden gespeichert (z. B. nicht die URL oder die Inhaltsdaten); eine Zweckverwendung nach § 113c TKG darf nur bei Verdacht besonders schwerer Straftaten erfolgen.[291] Es ist umstritten, ob die Eingriffsintensität der anlasslosen Speicherung einer Vielzahl von Daten durch die anderen Faktoren, also durch strenge Abrufmechanismen, gemindert werden kann.[292]

b) Zugriff auf Daten

Der Gesetzgeber wollte die Eingriffsintensität der anlasslosen Speicherung von Daten durch strenge Abrufmechanismen flankieren. Eine anlasslose Speicherung rechtfertigt sich vor allem über die enge Zweckbegrenzung des § 113c TKG zur Verfolgung besonders schwerer Straftaten im Rahmen der Ermittlung. Die nach § 113b TKG gespeicherten Daten dürfen nur für die drei folgenden Zwecke verwendet werden (§ 113c TKG): Erstens dürfen die Speicherungsverpflichteten die Daten an eine Strafverfolgungsbehörde übermitteln, soweit diese die Übermittlung unter Berufung auf eine gesetzliche Bestimmung verlangt, die ihr eine Erhebung der in § 113b TKG genannten Daten zur Verfolgung besonders schwerer Straftaten erlaubt. Dazu dient § 100g StPO als eine Ermächtigungsgrundlage. Zweitens

289 OVG NRW, 13 B 238/17, Beschluss am 22. Juni 2017.

290 Der Gesetzgeber spricht insoweit von einer „Vielzahl von Kritikpunkten, die in ihrer Gesamtbetrachtung die Unverhältnismäßigkeit bedeuteten“ und einer „Kombination“ von langer Speicherdauer ohne Differenzierung nach Datenart, vgl. BT-Drs. 18/5088, S. 23.

291 *Dalby*, Vorratsdatenspeicherung – Endlich?!, KriPoZ 2016, 113, 115.

292 Bejahend *Dalby*, Vorratsdatenspeicherung – Endlich?!, KriPoZ 2016, 113, 116; kritisch dazu *Roßnagel*, Die neue Vorratsdatenspeicherung – der nächste Schritt im Ringen um Sicherheit und Grundrechtsschutz, NJW 2016, 533, 538.

dürfen die Daten an eine Gefahrenabwehrbehörde der Länder übermittelt werden. Die Übermittlung soll sich dabei aus einer gesetzlichen Bestimmung begründen, die der Behörde eine Erhebung der in § 113b TKG genannten Daten zur Abwehr einer konkreten Gefahr für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes erlaubt. Der Erbringer öffentlich zugänglicher Telekommunikationsdienste darf schließlich die Daten zum Ersuchen der Bestandsdaten über eine IP-Adresse gemäß § 113 Abs. 1 Satz 3 TKG verwenden.[293] Eine Verwendung für andere Zwecke als die oben genannten ist nach § 113c Abs. 2 TKG explizit verboten. Es soll angesichts des Forschungsziels dieser Arbeit nachfolgend nur in die Verwendung des Strafverfolgungszweckes Einblick genommen werden. Dabei ermächtigt § 100g StPO die Strafverfolgungsbehörden mit dem bestimmten Straftatbezug unter einigen Voraussetzungen, Verkehrsdaten zu erheben.

§ 100g StPO unterscheidet mehrere Arten von Auskünften: § 100g Abs. 1 Satz 1 regelt die allgemeine Auskunft über die gemäß § 96 TKG gespeicherten Daten zur Aufklärung einer Straftat von erheblicher Bedeutung bzw. mittels Telekommunikation. § 100g Abs. 1 Satz 3 StPO betrifft speziell die Erhebung von Standortdaten als einer Sonderform von Verkehrsdaten nur für künftig anfallende Verkehrsdaten oder in Echtzeit, die unabhängig von der Vorratsdatenspeicherung gespeichert werden – weil die Vorratsdatenspeicherung auf den Zugriff auf die bereits beim Anbieter vorsorglich gespeicherten Daten abzielt. § 100g Abs. 2 StPO normiert den strafprozessualen Zugriff auf die gemäß § 113b TKG gespeicherten Verkehrsdaten (Vorratsdatenspeicherung) und § 100g Abs. 3 StPO gestaltet schließlich eine Funkzellenabfrage, also die Erhebung aller in einer Funkzelle angefallenen Verkehrsdaten.

Die unabhängig von der Vorratsdatenspeicherung nach § 96 TKG gespeicherten Verkehrsdaten dürfen nur dann erhoben werden, wenn bestimmte Tatsachen einen Verdacht begründen, dass eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 StPO bezeichnete Straftat (Verdacht auf schwere Straftaten, die eine Telekommunikationsüberwachung auslösen können) oder eine Straftat mittels Telekommunikation begangen wurde, soweit dies für die Erforschung des Sachverhalts erforderlich ist und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Für die Straftat mittels Telekommunikation wird gefordert, dass die Erforschung des Sach-

293 BVerfGE 125, 260 (340 f.); dazu kritisch *Roßnagel/Moser-Knierim/Schweda*, Interessenausgleich in der Vorratsdatenspeicherung, S. 13 ff.

verhalts auf andere Weise aussichtslos wäre. Für den Verdacht bezüglich einer Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere einer in § 100a Abs. 2 StPO bezeichneten Straftat (Straftatenkatalog) oder einer Straftat mittels Telekommunikation ist zur Erhebung von Verkehrsdaten die Erforderlichkeit und die Verhältnismäßigkeit vorauszusetzen. Für die Erhebung von Verkehrsdaten beim Verdacht einer Straftat mittels Telekommunikation wird außerdem die Subsidiarität der Aussichtslosigkeit auf andere Weise gefordert. Die Erhebung von Standortdaten darf nur für künftig anfallende Verkehrsdaten oder in Echtzeit und nur zum Ziel der Erforschung des Sachverhalts oder der Ermittlung des Aufenthaltsortes des Beschuldigten geschehen. Dies beschränkt sich zudem auf den Fall des § 100g Abs. 1 Satz 1 Nr. 1 StPO, also darauf, dass bestimmte Tatsachen einen Verdacht begründen, dass jemand eine Straftat von auch im Einzelfall erheblicher Bedeutung begangen hat.

Die nach § 113b TKG im Rahmen der Vorratsdatenspeicherung gespeicherten Daten dürfen gemäß § 100g Abs. 2 StPO unter relativ strengen Voraussetzungen erhoben werden.[294] Bei der Erhebung von Verkehrsdaten gemäß Art. 100g Abs. 2 StPO wird davon ausgegangen, dass die Daten tatsächlich gespeichert wurden, sodass nur die Verkehrsdaten der Vergangenheit erfasst werden. Für die Erhebung zukünftig anfallender Verkehrsdaten oder zur Erhebung in Echtzeit ist diese Vorschrift hingegen nicht einschlägig. Gegenstand der Auskunft nach Abs. 2 sind die Verbindungsdaten nach § 113b Abs. 2 TKG bezüglich Telefondiensten, diejenigen nach § 113b Abs. 3 TKG bezüglich Internetzugangsdiensten und die Standortdaten nach § 113b Abs. 4 TKG bezüglich Funkzellen.[295] Retrograde Standortdaten dürfen nach Ablauf der Überleitungsvorschrift des § 12 EGStPO zum 29. Juli 2017 nur auf Grundlage von Abs. 2 i. V. m. § 113b TKG erhoben werden.[296] Da die Speicherverpflichtung nach den §§ 113b bis 113e und 113g spätestens ab dem 1. Juli 2017 zu erfüllen sind, dürfen die nach § 96 Abs. 1 Satz 1 Nr. 1 TKG gespeicherten Standortdaten auf der Grundlage des § 100g Abs. 1 a. F. erhoben werden, damit in der Zwischenzeit ein Abruf gespeicherter Standortdaten möglich bleibt.

Für die Erhebung der nach Vorratsdatenspeicherung gespeicherten Daten genügt ein einfacher Verdacht einer besonders schweren Straftat im Sinne des Abs. 2 Satz 2. Den Tatverdacht müssen aber bestimmte Tatsa-

294 Über die unterschiedlichen Voraussetzungen je nach der Datenart siehe unten Tabelle 2.

295 Vgl. *Bär*, BeckOK-TKG, § 113b, Rn. 5 ff., 15, 16 ff.

296 BGH, Ermittlungsrichter, 03.08.2017 – 1 BGs 237/17.

chen begründen.[297] Dieser muss also objektivierbar und konkret auf den Einzelfall bezogen sein.[298] Mit Blick auf das Gewicht des Grundrechtseingriffs durch den Zugriff auf die nach § 113b TKG gespeicherten Daten muss sich der Verdacht auf eine hinreichende Tatsachenbasis stützen und mehr als nur unerheblich sein.[299] Für die Erhebung dieser Daten schließt § 100g Abs. 2 StPO einen bestimmten Straftatenkatalog an. Nur wenn ein Verdacht begründet wird, dass eine der in § 100g Abs. 2 StPO aufgezählten Straftaten begangen wurde und die Tat auch im Einzelfall besonders schwer wiegt, dürfen die nach § 113b TKG gespeicherten Daten erhoben werden. Der Katalog ist dabei abschließender Natur. Im Deliktskatalog in Abs. 2 Satz 2 spiegelt sich die Erforderlichkeit der Ermittlung über den Zugriff auf die Vorratsdaten. Der Gesetzgeber hat im Hinblick auf die hohe Grundrechtsrelevanz des Abrufs verpflichtend gespeicherter Daten den Katalog im Vergleich zu dem in § 100a Abs. 2 Satz 2 deutlich reduziert.[300] Dieser Katalog stößt wegen seines Umfangs aber oft auf Kritik: Einerseits seien manche Deliktsbereiche vom Katalog des § 100g Abs. 2 Satz 2 nicht erfasst, obwohl polizeiliche Strukturermittlungen ohne Vorratsdatenspeicherung kaum sinnvoll durchgeführt werden können, z. B. im Bereich der Organisierten Kriminalität der gewerbsmäßige Betrug gemäß § 263 Abs. 3 Satz 2 Nr. 1 StGB.[301] Andererseits seien einige Delikte konsequenterweise aus dem Katalog des Absatzes 2 Satz 2 zu streichen, weil für die Delikte kaum eine kriminalistische Notwendigkeit des Zugriffs auf die Vorratsdaten besteht, wie etwa beim besonders schweren Fall des Landfriedensbruchs nach § 125a StGB.[302] Es wird außerdem der Vorwurf erhoben, dass der Bezug auf die im Katalog des Absatzes 2 Satz 2 aufgeführten Grundtatbestände zu Beginn eines Ermittlungsverfahrens in der Regel nicht festgestellt wird und sich auch die Möglichkeit eines (besonders) schweren Falls erst im Laufe des Ermittlungsverfahrens herausstellen kann;

297 Vgl. BVerfGE 107, 299; *Bruns*, KK-StPO, § 100a Rn. 30; *Hauck*, LR-StPO, § 100a Rn. 42.

298 *Hauck*, LR-StPO, § 100g Rn. 11.

299 BGH, NStZ-RR 2016, 346, Rn. 9.

300 BT-Drs. 18/5088, S. 32.

301 *Hauck*, LR-StPO, § 100g Rn. 48. Ebenso für eine maßvolle Erweiterung des Katalogs Münch ZRP 2015 130; *Herrmann*, Vorratsdatenspeicherung ist notwendig, in: *Hanns Seidel Stiftung* (Hrsg.), Politische Studien Bd. 458 im Fokus „Frei oder Sicher? – brauchen wir die Vorratsdatenspeicherung?" 14 (17); ablehnend aber *Leutheusser-Schnarrenberger*, Die Beerdigung 1. Klasse der anlasslosen Vorratsdatenspeicherung in Europa, DuD 2014, 589, 590 f.

302 *Hauck*, LR-StPO, § 100g, 49; Deutscher Richterbund (Stellungnahme), 2 f.

obwohl Verkehrsdaten als Ermittlungsansatz vor allem zu Beginn eines Ermittlungsverfahrens von großer Bedeutung sind.[303]

Wie in § 100a StPO ist der Einsatz dieser Maßnahme in § 100g Abs. 2 nur zulässig, soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre. Im Vergleich mit den Erfolgsaussichten anderer Maßnahmen ist bei gleichen Voraussetzungen die schonendere Maßnahme zu ergreifen.

Außerdem erfordern die Auskünfte nach Abs. 2, dass die Datenerhebung in einem angemessenen Verhältnis zur Bedeutung der Sache steht. Bei staatlichen Grundrechtseingriffen ist ungeachtet der vom Gesetz vorgesehenen generellen Eingriffsvoraussetzungen die Überprüfung der verfassungsrechtlichen Verhältnismäßigkeit grundsätzlich vorausgesetzt. § 100g Abs. 2 erwähnt trotz des allgemeinen Grundsatzes der Verhältnismäßigkeit zusätzlich ein angemessenes Verhältnis zur Bedeutung der Sache. Die Bedeutung dieser Klausel erklärt der Gesetzgeber in seinem Gesetzesentwurf jedoch nicht. Die Klausel ist als eine zweite, gesonderte Verhältnismäßigkeitsprüfung im Licht der Anforderungen des EuGH zu verstehen, wonach der Schutz des Grundrechts auf Achtung des Privatlebens verlangt, dass sich die Ausnahmen vom Schutz personenbezogener Daten auf das absolut Notwendige beschränken müssen.[304] Bei der Angemessenheitsprüfung im Rahmen der ursprünglichen Verhältnismäßigkeitsprüfung ist eine Abwägung sämtlicher Vor- und Nachteile der Maßnahme vorzunehmen. Eine Maßnahme ist also nur dann verhältnismäßig im engeren Sinn, wenn die Nachteile, die mit der Maßnahme verbunden sind, nicht völlig außer Verhältnis zu den Vorteilen stehen, die sie bewirkt. In der Klausel des angemessenen Verhältnisses zur Bedeutung der Sache ist daher eine Garantie zu sehen, die bei der hohen Eingriffsintensität einer vorrätigen Speicherung personenbezogener Daten vieler Personen einen wirksamen Schutz dieser Daten vor Missbrauch sowie vor jedem unbefugten Zugang zu diesen Daten und jeder unberechtigten Nutzung ermöglicht.[305] Es lässt sich feststellen, dass den möglichen Bedenken hinsichtlich der hohen Eingriffsintensität der Maßnahme, des drohenden Vertrauensverlusts in die

303 *Hauck*, LR-StPO, § 100g, 50.
304 EuGH, Urteil vom 8. April 2014 in den Rechtssachen C-293/12, C-594/12.
305 So *Schmitt*, Strafprozessordnung, § 100g Rn. 35; *Bär*, BeckOK-StPO, § 100g Rn. 18; *Moser-Knierim*, Vorratsdatenspeicherung – Zwischen Überwachungsstaat und Terrorabwehr, S. 257.

Strafjustiz und der Missbrauchsanfälligkeit[306] mit der Verhältnismäßigkeit der Maßnahme in besonderem Maße begegnet wird.

§ 100g StPO enthält darüber hinaus in Abs. 3 eine Sonderregelung zu der Funkzellenanfrage. Bei einer solchen Abfrage werden alle Verkehrsdaten erhoben, die in einer bestimmten Funkzelle angefallen sind, um festzustellen, welche Mobilgeräte zu einer bestimmten Zeit der betreffenden Funkzelle zuzuordnen waren.[307] Die Maßnahme kommt in Betracht, wenn Kennungen nicht bekannt sind, aber Erkenntnisse dafür vorliegen, dass in bestimmten räumlichen Bereichen mit Hilfe des Mobilfunks Telekommunikation betrieben wurde, deren Daten für die Identifizierung noch unbekannter Täter[308] von Bedeutung sein könnten. Da Gegenstand dieser Maßnahme alle Verkehrsdaten sind, die in einer bestimmten Funkzelle angefallen sind, ist die Gefahr, dass Telekommunikationsdaten völlig unbeteiligter Personen erhoben werden, sehr groß. Der Gesetzgeber begegnet daher den vielen Bedenken[309] hinsichtlich der Verfassungsmäßigkeit, insbesondere der Verhältnismäßigkeit der Maßnahme, mit engen Voraussetzungen: Während bei Funkzellenabfragen[310] nach § 100g Abs. 3 StPO die Erhebung von nach § 96 Abs. 1 TKG gespeicherten Verkehrsdaten zulässig ist, wenn die Voraussetzungen des § Abs. 1 Satz 1 Nr. 1 StPO vorliegen, die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht und die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert ist, müssen für eine Erhebung der nach § 113b TKG gespeicherten Verkehrsdaten für eine Funkzellenabfrage die Voraussetzungen des § 100g Abs. 2 erfüllt sein. Beim Einsatz der Maßnahme ist ferner

306 *Zimmer*, Zugriff auf Internetzugangsdaten: Unter besonderer Berücksichtigung der Verhältnismäßigkeit einer verdachtsunabhängigen Vorratsdatenspeicherung, 2012, S. 195 ff.

307 BT-Drs. 18/5088, S. 32.

308 *Hilger*, Gesetzgebungsbericht: §§ 100g, 100h StPO, die Nachfolgeregelungen zu § 12 FAG, GA 2002, 228, 230; *Wohlers/Demko*, Der strafprozessuale Zugriff auf Verbindungsdaten (§§ 100g, 100h StPO), StV 2003, 241, 247.

309 Vgl. *Singelnstein*, Verhältnismäßigkeitsanforderungen für strafprozessuale Ermittlungsmaßnahmen – am Beispiel der neueren Praxis der Funkzellenabfrage, JZ 2012, 601, 601 ff. m. w. N.; *Singelnstein*, Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen – Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co., NStZ 2012, 593, 602: „enorme Streubreite".

310 Die Funkzellenabfrage ist nach § 100g Abs. 3 Satz 1 StPO die Erhebung aller in einer Funkzelle angefallenen Verkehrsdaten und damit nicht auf die Erhebung von Standortdaten beschränkt (BT-Drs. 18/5088, S. 32).

davon auszugehen, dass überhaupt eine Verbindung zustande gekommen ist.[311]

Für den Zugriff auf die Daten, die der Anbieter der Telekommunikationsdienste gespeichert hat, werden grundsätzlich bestimmte Grundrechtseingriffsvoraussetzungen vorgesehen, etwa einfacher Verdacht einer Straftat von erheblicher Bedeutung bzw. einer besonders schweren Straftat, Subsidiaritätsklauseln und der Grundsatz der Verhältnismäßigkeit. Um die Daten, auf die die Strafverfolgungsbehörden zugreifen dürfen, zu erweitern, hat der Gesetzgeber die Zugriffsermächtigung verpflichtend gespeicherter Daten gemäß § 113b TKG eingeführt, wobei im Lichte der hohen Eingriffsintensität dieser Maßnahme die Voraussetzungen verstärkt wurden. So werden angesichts der schon weit im Vorfeld der Regelung vorgebrachten Bedenken und der Tatsache, dass die Maßnahme eine Vielzahl von Daten Unbeteiligter erfasst, zusätzlich eine Einschränkung auf die abschließenden Katalogtaten und eine besondere Verhältnismäßigkeitsprüfung gefordert.

§ 101a StPO, der unter dem neuen Vorratsdatenspeicherungsgesetz neu eingefügt wurde, regelt den Richtervorbehalt. Danach bedarf es für den Zugriff auf die Verkehrsdaten unter Berufung auf § 100g StPO grundsätzlich einer gerichtlichen Anordnung auf Antrag der Staatsanwaltschaft (§ 100b StPO). In den Fällen einer Auskunft über die nach § 96 TKG gespeicherten Daten besteht bei Gefahr im Verzug die Möglichkeit der Anordnung durch die Staatsanwaltschaft, wobei die Anordnung der Staatsanwaltschaft binnen drei Werktagen von einem Gericht bestätigt werden soll. Diese Möglichkeit wird in den Fällen des § 100g Abs. 2 StPO (Auskunft über die Vorratsdaten: Vorratsdatenspeicherung), auch in Verbindung mit § 100g Abs. 3 Satz 2, ausgeschlossen. Die Anordnung darf sich nur gegen den Beschuldigten oder gegen Personen richten, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss benutzt (§ 100a Abs. 3 StPO). In der Entscheidung sind anzugeben: der Name und die Anschrift des Betroffenen, gegen den sich die Maßnahme richtet; die Rufnummer oder eine andere Kennung des zu überwachenden Anschlusses oder des Endgerätes; Art, Umfang und Dauer der Maßnahme unter Benennung des Endzeitpunktes sowie die zu übermittelnden Daten und der Zeitraum, für den sie übermittelt werden sollen.

311 Für die Auskunft über die Daten nur auf Bereitschaft geschalteter Endgeräte gilt § 100a bzw. § 100i StPO.

Die Verwendung personenbezogener Daten, die durch Maßnahmen nach § 100g Abs. 2 StPO, auch in Verbindung mit § 100g Abs. 3 Satz 2, erhoben wurden, muss unter Zweckbindung stehen. Diese Zweckbindung bestimmt § 101a Abs. 4 StPO. Die Daten dürfen also in anderen Strafverfahren zur Aufklärung einer Straftat, auf Grund derer eine Maßnahme nach § 100g Abs. 2, auch in Verbindung mit § 100g Abs. 3 Satz 2, angeordnet werden könnte, oder zur Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person verwendet werden. Ihre Übermittlung darf zu Zwecken der Abwehr von konkreten Gefahren für Leib, Leben oder Freiheit einer Person oder für den Bestand des Bundes oder eines Landes geschehen.

Damit fordert § 100g StPO für die Erhebung der nach § 96 TKG gespeicherten Daten bei einem Verdacht für eine in § 100a bezeichnete Straftat auch im Einzelfall von erheblicher Bedeutung oder für eine Straftat mittels Telekommunikation die Erforderlichkeit der Maßnahme und die Verhältnismäßigkeit zwischen der Maßnahme und der Bedeutung der Sache. Für eine Datenanfrage bezüglich einer Straftat mittels Telekommunikation fügt das Gesetz jedoch die Anforderung „wenn die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre" hinzu. Die Erhebung von Standortdaten kann nicht nur bei der Erforderlichkeit für die Erforschung des Sachverhalts, sondern auch bei der Erforderlichkeit für die Ermittlung des Aufenthaltsortes des Beschuldigten ergriffen werden. Für die Funkzellenanfrage wird darüber hinaus gefordert, dass die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise aussichtslos oder wesentlich erschwert wäre. Im Gegensatz dazu wird die Erhebung der nach § 113b TKG gespeicherten Daten an engere Voraussetzungen geknüpft: wenn bestimmte Tatsachen den Verdacht für eine in § 100g Abs. 2 bezeichnete Straftat begründen und die Tat auch im Einzelfall besonders schwer wiegt und soweit die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre und die Erhebung der Daten in einem angemessenen Verhältnis zur Bedeutung der Sache steht.

Trotz dieser Unterschiede in den Anforderungen haben die Maßnahmen nach § 100a und § 100g Abs. 1 bis 3 einige Gemeinsamkeiten. Für sämtliche Auskünfte nach § 100g ist der Anfangsverdacht einer bestimmten Straftat vorausgesetzt. Es genügt ein einfacher Verdacht, der auf bestimmten Tatsachen beruhen muss, also objektivierbar und konkret auf den

Einzelfall bezogen sein muss,[312] einer Straftat von erheblicher Bedeutung bzw. einer besonders schweren Straftat. Insofern entspricht die gesetzliche Regelung der in § 100a. Alle drei Auskunftsformen des § 100g fordern eine Subsidiarität, indem die Maßnahme für die Erforschung des Sachverhalts und/oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich sein muss oder die Erforschung bzw. Ermittlung auf andere Weise aussichtslos oder wesentlich erschwert wäre. Mit den Subsidiaritätsvorschriften betont § 100g ebenso wie die Telekommunikationsüberwachung in § 100a den Verhältnismäßigkeitsgrundsatz noch einmal, weil der Eingriff schon rechtswidrig wäre, wenn der verfolgte Zweck mit für die Betroffenen weniger belastenden Mitteln erreichbar wäre.[313] Darüber hinaus gelten der Richtervorbehalt, die Benachrichtigungspflicht und die Anordnung nur gegen den Beschuldigten oder gegen Personen, von denen auf Grund bestimmter Tatsachen anzunehmen ist, dass sie für den Beschuldigten bestimmte oder von ihm herrührende Mitteilungen entgegennehmen oder weitergeben oder dass der Beschuldigte ihren Anschluss oder ihr informationstechnisches System benutzt, ebenso wie in § 100a auch für die Auskunftsformen in § 100g.

Der Straftatkatalog nach § 100g Abs. 2 StPO ist aber angesichts der Eingriffsintensität enger als die Katalogtaten nach § 100a Abs. 2 gefasst. Nach der Entscheidung des Bundesverfassungsgerichts, die besagt, dass ein Datenabruf zumindest den durch bestimmte Tatsachen begründeten Verdacht einer schweren Straftat voraussetzt und eine Generalklausel oder lediglich der Verweis auf Straftaten von erheblicher Bedeutung hingegen nicht ausreichen würden, hat der Gesetzgeber einen Katalog besonders schwerer Straftaten für die Erhebung der nach § 113b TKG gespeicherten Daten geschaffen.

Die Verfahren der Datenübermittlung, die auf Verlangen einer zuständigen Stelle erfolgen, bestimmen die Rechtsverordnung nach § 110 Abs. 2 TKG und die Technische Richtlinie nach § 110 Abs. 3 TKG (§ 113c TKG).

312 BT-Drs. 14/7008, S. 6; *Wohlers/Demko*, Der strafprozessuale Zugriff auf Verbindungsdaten (§§ 100g, 100h StPO), StV 2003, 241, 245.

313 BT-Drs. 14/7008, S. 7; BVerfGE 107, 299.

Tabelle 2: Voraussetzungen je nach gespeicherter Datenart

	Straftatbezug	Voraussetzungen
Die nach § 96 TKG gespeicherten Daten	Alt. 1: Verdacht auf eine in § 100a Abs. 2 StPO bezeichnete Straftat von auch im Einzelfall erheblicher Bedeutung	– soweit dies für die Erforschung des Sachverhaltes erforderlich ist und – die Erhebung in einem angemessenen Verhältnis zur Bedeutung der Sache steht.
	Alt. 2: Verdacht auf eine Straftat mittels Tele-kommunikation	– soweit dies für die Erforschung des Sachverhaltes erforderlich ist, – die Datenerhebung in einem angemessenen Verhältnis zur Bedeutung der Sache steht und – die Erforschung des Sachverhalts auf andere Weise aussichtslos wäre.
Die nach § 113b gespeicherten Daten	Verdacht auf eine der in § 113b Abs. 2 Satz 2 bezeichneten *besonders schweren Straftaten*, die auch im Einzelfall besonders schwer wiegt	– soweit die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre und – die Datenerhebung in einem angemessenen Verhältnis zur Bedeutung der Sache steht.
künftig anfallende Standortdaten oder in Echtzeit	Verdacht für eine in § 100a Abs. 2 StPO bezeichnete Straftat von auch im Einzelfall erheblicher Bedeutung	soweit dies für die Erforschung des Sachverhaltes erforderlich ist

Funkzellenanfrage: alle in einer Funkzelle angefallenen Verkehrsdaten	Verdacht für eine in § 100a Abs. 2 StPO bezeichnete Straftat von auch im Einzelfall erheblicher Bedeutung	– soweit die Datenerhebung in einem angemessenen Verhältnis zur Bedeutung der Sache steht und – die Erforschung des Sachverhaltes oder die Ermittlung des Aufenthaltsortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.
§ 100a	Verdacht für eine in § 100g Abs. 2 StPO bezeichnete *schwere* Straftat	– wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthalts-ortes des Beschuldigten auf andere Weise wesentlich erschwert oder aussichtslos wäre.

c) Löschungspflicht

Im TKG ist nicht nur die Speicherungsermächtigung bestimmter Daten durch den Diensteanbieter für die unverzügliche Beantwortung von Auskunftsersuchen berechtigter Stellen geregelt. Vielmehr bestimmt es auch deutlich die Löschungspflicht dieser Daten zum Schutz personenbezogener Daten durch das Datensparsamkeitsprinzip entsprechend der verfassungsrechtlichen Verpflichtung, die Daten nach Ablauf der Höchstdauer der Speicherfrist zu löschen.[314] Während die alte Regelung zur Vorratsdatenspeicherung eine einheitliche Speicherdauer der Daten von sechs Monaten vorsah, fordert § 113b TKG n. F. zwei unterschiedliche Möglichkeiten der Speicherfrist der nach §§ 113a und b TKG gespeicherten Daten. Auf diese Weise berücksichtigt die Vorschrift die Unterschiede hinsichtlich Umfang und Bedeutung der durch die Vorratsdatenspeicherung geschaffenen Datenbestände. Daten nach § 113b Abs. 2 und 3 sind von Erbringern öffentlich zugänglicher Telefondienste sowie Internetzu-

314 BVerfGE 125, 260 (333).

gangsdienste für zehn Wochen zu speichern, Standortdaten nach Abs. 4 hingegen für vier Wochen. Die Löschung muss gemäß § 113b Abs. 9 TKG unverzüglich, spätestens jedoch innerhalb einer Woche nach Ablauf der Speicherfristen erfolgen. Dabei muss die Löschung irreversibel sein. Darunter versteht man, dass sichergestellt werden muss, dass auf den Speichermedien physikalisch keine Fragmente oder gar noch die gesamten Daten vorhanden sind und etwa mit technischen Mitteln wieder rekonstruiert werden können. Die irreversible Löschung der Daten muss daher nach dem Stand der Technik gewährleistet werden, weshalb dazu in den Anforderungskatalog nach § 113f entsprechende Regelungen aufzunehmen sein werden.[315] Die Löschung ist gemäß § 113e Abs. 1 Satz 1 aktenkundig zu machen.

Anders als bei der Rasterfahndung ist bei der Vorratsdatenspeicherung die Löschung oder die Rückgabe der vom Diensteanbieter übermittelten Daten nicht vorgesehen. Der Grund hierfür liegt darin, dass für die Verwendung der nach § 100g StPO i. V. m. § 113b TKG gewonnenen Daten eine enge Zweckbegrenzung vorgesehen ist. Dabei stellt § 113c Abs. 1 Nr. 1 und 2 TKG die Voraussetzung der Datenübermittlung dar und § 113c Abs. 2 TKG schließt die Datenverwendung für andere als die in § 113c Abs. 1 TKG genannten Zwecke ausdrücklich aus. In diesem Zusammenhang muss eine hinreichende Erörterung der Eignung der Maßnahme zur Ermittlung im Anordnungsbeschluss angegeben sein.

d) Mitteilungspflicht

Nach § 101a Abs. 6 StPO sind die Beteiligten der betroffenen Telekommunikation grundsätzlich von der Erhebung der Verkehrsdaten nach § 100g StPO zu benachrichtigen, weil § 100g grundsätzlich eine offene Ermittlungsmaßnahme darstellt.[316] Da Verkehrsdaten in der Praxis regelmäßig bereits zu einem frühen Zeitpunkt erhoben werden, zu dem die Ermittlungen noch heimlich geführt werden, ist allerdings davon auszugehen, dass der offene Zugriff die Ausnahme bleiben wird.[317] Im Hinblick auf den Inhalt und die Zuständigkeit für die Benachrichtigung gelten nach Abs. 6 Satz 2 Halbsatz 1 die Regelungen des § 101 Abs. 4 Satz 2 bis 5 und Abs. 5 bis 7 entsprechend. Nach § 101 Abs. 7 StPO ist auf die Möglichkeit

315 *Bär*, BeckOK-TKG, § 113b TKG Rn. 26.
316 BT-Drs. 18/5088, S. 36.
317 *Gercke*, HK-StPO, § 101a Rn. 25 m. w. N.

nachträglichen Rechtsschutzes und die dafür vorgesehene Frist hinzuweisen. Die Benachrichtigung muss sich insbesondere auf die Anordnung und Durchführung einschließlich der Dauer und des Umfangs der Maßnahme erstrecken. Die Benachrichtigung unterbleibt, wenn ihr überwiegende schutzwürdige Belange einer betroffenen Person entgegenstehen (§ 101 Abs. 4 Satz 3 StPO). Die Benachrichtigung kann zurückgestellt werden, soweit sie den Untersuchungszweck gefährden würde (§ 101 Abs. 5 Satz 1 StPO). Das Unterbleiben oder die Zurückstellung der Benachrichtigung bedarf dabei der Anordnung des zuständigen Gerichts (§ 101a Abs. 6 Satz 2 Nr. 1 und 2 StPO). Die Zurückstellung der Benachrichtigung ist erstmalig auf höchstens zwölf Monate zu befristen und kann durch das Gericht verlängert werden. Das Gericht kann dem endgültigen Absehen von der Benachrichtigung zustimmen, wenn die Voraussetzungen für eine Benachrichtigung mit an Sicherheit grenzender Wahrscheinlichkeit auch in Zukunft nicht eintreten werden (§ 101 Abs. 6 StPO). Insoweit bedarf es einer Begründung im Einzelfall.[318]

318 BT-Drs. 18/5088, S. 36.

Teil 3: Landesbericht USA

A. Der verfassungsrechtliche Datenschutz

I. Privacy Protection und Datenschutz

1. Privacy Protection

Das Recht auf *privacy* ist in der US-Verfassung nicht ausdrücklich als ein Recht genannt. Der Begriff „privacy" ist insgesamt schwer zu definieren, da seine Bedeutung vielfach je nach Kontext und der Art und Weise des Gebrauchs variiert und dadurch vage ist.[319] In vielen Ansätzen wurde ver-

---

319 Während die Bedeutung des Begriffs der *privacy* wie oben angeführt relativ vage ist, hat der Begriff der Privatsphäre in der deutschen Rechtsordnung eine auf die verschiedenen Rechtsgebiete übergreifende, relativ einheitliche Bedeutung. Der Begriff der *privacy* wurde durch die Rechtsprechung entwickelt, nachdem Gerichte auf der Ebene des Bundesstaaten *four privacy torts* im Deliktsrecht anerkannt haben: (1) *Intrusion upon Seclusion* (Restatement (Second) of Torts § 652B (1977), this tort allows plaintiffs to seek remedy for the invasion of their „solitude or seclusion" or „private affairs or concerns" if the intrusion is „highly offensive to a reasonable person"); (2) *False Light* (Restatement (Second) of Torts § 652E (1977), this tort allows plaintiffs to seek remedy when they are portrayed in a false light that is „highly offensive to a reasonable person" because the defendant publicly disclosed certain matters or information); (3) *Public Disclosure of Private Facts* (Restatement (Second) of Torts § 652D (1977), this tort allows plaintiffs to seek remedy for the disclosure of a private fact that is „highly offensive to a reasonable person" and not about a matter of public concern); and (4) *Appropriation* (Restatement (Second) of Torts § 652C (1977), this tort allows plaintiffs to seek remedy when their „name or likeness" is appropriated for the defendant's „use of benefit"). Das Restatement of (Second) of Torts versteht unter dem Recht auf *privacy* das Interesse des Einzelnen an der Abgeschiedenheit (unreasonable intrusion upon the seclusion of another) und der Vermeidung der Verwendung seines Namens o. Ä. (appropriation of the other's name or likeness), der unbegründeten Publizität seines privaten Lebens (unreasonable publicity given to the other's private life) sowie der Publizität, die ihn unbegründet in ein falsches Licht der Öffentlichkeit stellt (publicity that unreasonably places the other in a false light before the public). Obwohl die frühzeitige Erfassung des Begriffs der *privacy* durch den US-amerikanischen Obersten Gerichtshof (U. S. Supreme Court) dem Begriff „Privatsphäre" in der deutschen Rechtsordnung nicht zu entsprechen scheint und auch keine Ähn-

sucht, die Bedeutung von *privacy* zu definieren. Ein Entwurf der *privacy* beruhte auf dem „Recht, in Ruhe gelassen zu werden (*the right to be let alone*)", das in der von Richter *Cooley* im Jahr 1880 im Rahmen des Deliktsrechts veröffentlichten Abhandlung formuliert wurde. Zu dieser Zeit wurde der Ausdruck des Rechts auf *privacy* aber noch nicht unmittelbar benutzt.[320] Anlass zu erneuten heftigen Diskussionen um das Thema gab der Aufsatz *The Right to Privacy*,[321] den Samuel D. Warren und Louis D. Brandeis 1890 veröffentlichten. In diesem Aufsatz wird das Thema folgendermaßen erörtert: „Jedem stehen die Sphären von Gedanken, Meinungen und Gefühlen zu, die dann in dem gleichen Maße wie bei Körperverletzungen verletzt werden, wenn seine persönlichen Angelegenheiten öffentlich bekannt gegeben werden."[322]

Der Supreme Court führte in seiner *Griswold v. Connecticut*-Entscheidung aus, dass das Recht auf *privacy* in den Penumbras und Emanationen anderer verfassungsmäßiger Schutzmaßnahmen zu finden sei, wie etwa der Selbstbelastungsklausel des fünften Verfassungszusatzes, obwohl die *Bill of Rights* den Begriff der *privacy* nicht explizit erwähnt. Damit entschied das Gericht, dass die US-Verfassung durch die *Bill of Rights* ein Grundrecht auf *privacy* beinhaltet.[323] Die Rechte, die aus diesen von der Entsprechung als

---

lichkeit zur Idee der informationellen Selbstbestimmung oder dem Datenschutz besteht, scheint die Übersetzung von „privacy" mit „Privatsphäre" deshalb zutreffend zu sein, weil das *Restatement of Torts* den Begriff der *privacy* so ähnlich fasst wie der Begriff „"Privatsphäre" im deutschen Recht verwendet wird und weil die Erfassung des Supreme Courts mit der Zeit erweitert wird und sogar „Information Privacy" im Kontext der *privacy* diskutiert wird.

320 *Cooley*, A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract, 2nd ed., 1888: "The right to one's person may be said to be a right of complete immunity: to be let alone."

321 *Warren/Brandeis*, The Right to Privacy, Harvard Law Review, Vol. 4, No. 5., 1890, 193.

322 *Warren/Brandeis*, The Right to Privacy, Harvard Law Review, Vol. 4, No. 5., 1890, 193, 205: "These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. It is like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed."

323 Der US-amerikanische Supreme Court hat erst in der *Griswold*-Entscheidung anerkannt, dass sich das verfassungsrechtliche Recht auf *privacy* im Halbschatten (Penumbra) und der Ausstrahlung (Emanation) einiger Verfassungszusätze – Art. 1, 3, 4, 5 und 9 – befindet (Griswold v. Connecticut, 381 U. S. 479 (484)).

Ursprung für die *privacy* genannten Verfassungszusätzen erfasst werden, stehen im Hinblick auf den bedeutenden und umfassenden Schutz der *privacy* jedoch weitaus stärker hinter den Rechten des vierten Verfassungszusatzes zurück und bieten somit keinen allgemein verbindlichen und verlässlichen Schutz. Es soll daher bei der Untersuchung des Privatsphären- und Datenschutzes der vierte Verfassungszusatz im Vordergrund stehen, der ein staatliches Organ dazu ermächtigt, den Lebensraum des Einzelnen zu durchsuchen und seine Sachen in Beschlag zu nehmen. In der *Boyd v. United States*-Entscheidung brachte der Supreme Court den vierten Verfassungszusatz und das Recht auf *privacy* in einen unmittelbaren Zusammenhang.[324] Der vierte Verfassungszusatz wurde eigentlich in Verbindung mit der Due-process-Anforderung des fünften Verfassungszusatzes berücksichtigt.[325] Der grundsätzliche Schutz gegen die staatliche rechtswidrige Nutzung der Technik stammt also aus dem vierten Verfassungszusatz, der dem Schutz des Einzelnen gegen unbegründete Durchsuchungen und Beschlagnahmungen dient.

Das Recht auf *privacy* wird von der Rechtsprechung im Kontext des vierten Verfassungszusatzes zunehmend erweitert anerkannt und steht damit in einer Konkretisierung seiner Konturen. Der Verfasser des vierten Verfassungszusatzes interessierte sich primär für die körperlichen Durchsuchungen von Personen, Häusern, Papieren und Vermögenswerten.[326] Dement-

---

324 *De Busser*, Data Protection in EU und USA Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters Between Judicial and Law Enforcement Authorities, S. 223; Boyd v. United States, 116 U. S. 616 (630): "constitutional liberty and security apply to all invasions on the part of the government and its employees of the sanctity of a man's home and the privacies of life. It is not the breaking of his doors and the rummaging of his drawers that constitutes the essence of the offence, but it is the invasion of his indefeasible right of personal security, personal liberty, and private property, where that right has never been forfeited by his conviction of some public offence."

325 Das erklärte der Richter Joseph P. Bradley in der *Boyd v. United States*- Entscheidung: "They throw great light on each other. For the 'unreasonable searches and seizures' condemned in the fourth amendment are almost always made for the purpose of compelling a man to give evidence against himself, which in criminal cases is condemned in the fifth amendment; and compelling a man 'in a criminal case to be a witness against himself', which is condemned in the fifth amendment, throws light on the question as to what is an 'unreasonable search and seizure' within the meaning of the fourth amendment." (Boyd v. United States, 116 U. S. 616 (633)).

326 Drapper v. United States, 358 U. S. 307.

sprechend entschied der Supreme Court im *Olmstead*-Fall,[327] in dem es um die Verfassungskonformität staatlicher Abhörmaßnahmen bei privaten Fernsprechern ging, dass eine immaterielle Abhörmaßnahme nicht unter den Schutzgegenstand des vierten Verfassungszusatzes fällt. *Brandeis* äußerte eine hiervon abweichende Meinung und betonte, dass der Schutz der *privacy* auch bezüglich immateriellen Maßnahmen besteht.[328] Beispielsweise werden Wohnungen als wichtige private Lebensräume beim Privatsphärenschutz verfassungsrechtlich geschützt. Der Schutz des Lebensraums, der unter dem Privatsphärenschutz von großer Bedeutung ist, wurde zu Beginn lediglich am Maßstab eines unbegründeten physischen Betretens eines privaten Lebensraums im Kontext des vierten Verfassungszusatzes gemessen. Zum Lebensraum gehören Wohnungen, Büros oder auch Hotelzimmer.[329] Die Erfassung der Begriffe „unbegründete Eingriffe" und „privater Raum" durch die Rechtsprechung erfährt eine allmähliche Änderung. Den Zugriff auf Informationen innerhalb eines verfassungsrechtlich geschützten Lebensraums rechtfertigt ausschließlich eine gerichtliche Anordnung, eine Einwilligung eines Betroffenen oder bestimmte Umstände wie ein dringender Fall. Der Schutz des Brief-, Post- sowie Fernmeldegeheimnisses wird gegen eine unbegründete Durchsuchung und Beschlagnahme im Kontext des vierten Verfassungszusatzes gewährt. Bis zu diesem Zeitpunkt war der Schutzgegenstand auf etwas Materielles und auf Räume beschränkt. Dem entspricht der *Olmstead*-Fall, in dem der Schutz deshalb verneint wurde, weil die Informationen, die bei einem Telefonanruf ausgetauscht werden, nichts Materielles sind und ein Strom von elektronischen Impulsen kein Raum ist.[330] Dem Supreme Court wurde die Gelegenheit gegeben, den *Ex Parte Jackson*-Fall[331] hierauf anzuwenden. Das hat er je-

327 Olmstead v. United States, 277 U. S. 438.

328 Olmstead v. United States, 277 U. S. 438 (478 f.): Brandeis äußerte die abweichende Meinung, dass der Verfassungsgeber Amerikaner in ihrem Glauben, ihren Gedanken und Gefühlen schützen wolle, dass das Recht, in Ruhe gelassen zu werden (*the right to be let alone*) das umfassendste und würdigste Recht sei und dass es sich bei allem unbegründeten staatlichen Eindringen in die Privatsphäre um die Verletzung des vierten Verfassungszusatzes handle, unbenommen der eingesetzten Mittel.

329 Katz v. United States, 389 U. S. 347 (359).

330 Olmstead v. United States, 277 U. S. 438.

331 Ex Parte Jackson, 96 U. S. 727 (733): "Letters and sealed packages of this kind in the mail are as fully guarded from examination and inspection. […] The constitutional guaranty of the right of the people to be secure in their papers against unreasonable searches and seizures extends to their papers, thus closed against inspection, wherever they may be."

doch nicht getan. Nach der Entscheidung des Supreme Court würden die USA keine ähnliche Betreuung der telegraphischen oder telefonischen Mitteilung wie die der versandten versiegelten Briefe gewährleisten.[332] Die *Olmstead*-Entscheidung hat den Schutz der *privacy* im Sinne des vierten Verfassungszusatzes als streng materiellen Bereich verankert.

Demzufolge sah der Supreme Court ursprünglich nur im physischen Betreten des Raums einen Eingriff in den Raum und forderte damit den *due process* als einen Rechtfertigungsgrund, während er ein staatliches Handeln, das kein physisches Betreten ähnlich einer technisch unterstützten Beweiserhebung voraussetzt, ohne Einschränkungen erlaubte. Im *Olmstead*-Fall hat die Strafverfolgungsbehörde die Telefonleitung der Wohnungen und Arbeitsplätze von Verdächtigen überwacht und auf diese Weise einen Beweis gewonnen, der zur Verurteilung der Verdächtigen führte. Der Supreme Court erklärte das als keine verfassungswidrige Durchsuchung. Die gerichtliche Entscheidung gründete sich darauf, dass die Strafverfolgungsbehörde den verfassungsrechtlich geschützten Raum nicht physisch betreten hat und die Telefonleitung kein Teil der Wohnung oder des Büros sei.[333] Auch beim Diktaphon, mit dem ein gesprochener Text (einschließlich der Anrufe) innerhalb eines Raums ohne physisches Betreten aufgenommen und wiedergegeben werden kann, wird keine gerichtliche Anordnung zur Rechtfertigung gefordert.[334] Diese Logik führte in einem anderen Fall hingegen zu einer gegensätzlichen Schlussfolgerung. Im *Silvermann*-Fall entschied das Gericht, dass die Verwendung der *spike mike* ohne gerichtliche Anordnung einen unbegründeten Eingriff darstelle.[335] Denn die Polizisten seien in den verfassungsrechtlich geschützten Raum physisch eingetreten, indem sie das elektronische Gerät am Heizrohr der Wohnung des Angeklagten befestigten. Daraus lässt sich ableiten, dass das geschützte Rechtsgut nicht das Recht ist, vor staatlichen Eingriffen oder staatlicher Kenntnis über etwas, was in einer Wohnung geschieht, sicher zu sein, sondern der Raum als solcher.

Der Supreme Court war jedoch aus doppeltem Grund dazu gezwungen, seine Auffassung über den vierten Verfassungszusatz im Hinblick darauf zu ändern, was als verfassungsrechtlich geschützter Raum und als ein Ein-

---

332 Olmstead v. United States, 277 U. S. 438 (464).

333 Olmstead v. United States, 277 U. S. 438 (464 f.): Der Richter Taft führt aus, dass eine Abhörmaßnahme von elektronischen Informationen außerhalb eines privaten Raums dem Wesen nach etwas ganz Anderes als das physische Betreten eines Raums zum Zwecke einer Gesprächsabhörung sei.

334 Goldmann v. United States, 316 U. S. 129.

335 Silvermann v. United States, 365 U. S. 505.

griff darin angesehen werden soll: Da einerseits die Technik fortschreitet und der Staat in der Lage ist, auch ohne physisches Betreten in verfassungsrechtlich geschützte Sphären einzudringen, lässt sich die frühere gerichtliche Auffassung über den vierten Verfassungszusatz nicht mehr rechtfertigen. Andererseits wurde das verfassungsrechtliche Recht auf *privacy* vom Supreme Court ausdrücklich anerkannt[336] und verschiedene Ausprägungen der *privacy* wurden danach von der Rechtsprechung entwickelt.[337] Die Anerkennung des Rechts auf *privacy* durch den Supreme Court schuf eine neue Lage. Von der Rechtsprechung wurde nachfolgend konkretisiert und erweitert, was das Recht auf *privacy* umfasst.

Die Rechtsprechung, die sich beim Schutz des privaten Raums ursprünglich nur auf ein physisches Betreten des Raums durch staatliche Organe bezogen hatte, erfuhr in der *Katz*-Entscheidung eine wichtige Änderung. Das Gericht stimmte hier dem Widerspruch des Richters *Brandeis* in der *Olmstead*-Entscheidung[338] zu und stellte fest, dass der vierte Verfassungszusatz auch für das Abhören gilt. Der Richter *Harlan* etablierte in seiner zustimmenden Meinung im *Katz*-Urteil eine Überprüfung „der begründeten Erwartung auf *privacy*".[339] Der Supreme Court hat aus dem vierten Verfassungszusatz eine begrenzte Sphäre des verfassungsrechtlichen Schutzes des Rechts auf *privacy* abgeleitet: Das Recht auf *privacy* und Freiheit vor staatlichem Eindringen besteht überall dort, wo eine Person eine begründete Erwartung auf *privacy* (*reasonable expectation of privacy*) hat.[340] Ob es dabei ein physisches Betreten eines privaten Raums gibt, spielt keine bedeutende Rolle mehr. Der Supreme Court führte daher statt einer Prüfung eines physischen Betretens ein neues Kriterium ein: die begründete Erwartung auf *privacy*. Das Kriterium besteht aus zwei Teilen: zum einen aus einem subjektiven Teil, bei dem es darum geht, ob ein Einzelner eine Erwartung auf *privacy* hat *(personal agency)* und zum anderen aus einem objektiven Teil, wobei die Erwartung gesellschaftlich als begründet zu erkennen ist. In der *Katz*-Entscheidung hat *Katz* eine öffentliche Telefonkabine zum Glücksspielanruf benutzt, obwohl die Nutzung von Draht-Fernmeldeeinrichtungen zum Glücksspiel nach dem das *Federal*

336 Griswold v. Connecticut, 381 U. S. 479.
337 Das Kontrazeptionsrecht des Unverheirateten (Eisenstadt v. Baird, 405 U. S. 438), das Abtreibungsrecht (Roe v. Wade, 410 U. S. 113) und das Homosexualitätsrecht (Lawrence v. Texas, 539 U.S. 558) wurden als Ausprägungen des Rechts auf Privatsphäre bestätigt.
338 Zu seiner abweichenden Meinung siehe oben Fn. 328.
339 Katz v. United States, 389 U. S. 347 (360 f.).
340 Katz v. United States, 389 U. S. 347.

Statute verboten ist. Die Strafverfolgungsbehörde hatte an der Außenwand der Telefonkabine ein Abhörgerät befestigt, um Katz' Stimme beim Anruf aufzunehmen. Sie hatte so einen Beweis gewonnen, der zur Verurteilung von *Katz* führte. Die Behörde behauptete mit Verweis auf den *Olmstead*-Fall, dass es keine physische Beeinträchtigung gab und eine Telefonkabine deshalb keinen verfassungsrechtlich geschützten privaten Raum darstelle, weil ihre Nutzung von jedem wahrgenommen werden kann. Der Supreme Court lehnte die *Olmstead*-Entscheidung ab und entwarf eine neue Regelung, die besagt, dass der Einzelne das *Privacy*-Interesse im Kontext des vierten Verfassungszusatzes nicht in einem physischen Raum, sondern in der Geheimhaltung von bestimmten Informationen und Materialien hat. Nach dem Gericht waren das Schließen der Telefonkabinentür und die Bezahlung für den Anruf ausreichende Aktivitäten, um die Erwartung auf *privacy* zu begründen.[341] Die *Katz*-Entscheidung ist deshalb von Bedeutung, weil hierbei keine Unerreichbarkeit der Öffentlichkeit, sondern die begründete Erwartung auf Privatsphäre im Vordergrund steht und der Schutz des Rechts auf *privacy* damit nicht mehr von der räumlichen Sicht abhängt. Der vierte Verfassungszusatz bietet daher in dem Fall Schutz, in dem eine Person eine begründete Erwartung auf *privacy* hat. Er erfordert einen *warrant*, der durch einen *probable cause* gestützt wird, damit die Strafverfolgungsbehörden eine Durchsuchung durchführen können. Auf die Schutzgewährleistung durch den vierten Verfassungszusatz wirken einige Doktrinen ein, die seine Anwendung ausschließen können:

1. *Third Party Doctrine* – Wenn eine Person Informationen einmal an Dritte weitergibt, kann sie keine *privacy* für diese Informationen mehr erwarten.[342]
2. *Misplaced Trust Doctrine* – Eine Person hat keinen Schutz vor Verrat durch einen Informanten oder einen verdeckten Ermittler, da die Person die Verantwortung für die Gefahr des Verrats zu übernehmen hat.[343]
3. *Plain View Doctrine* – Wenn etwas als zwecklos betrachtet wird, handelt es sich nicht um eine Durchsuchung und löst keinen Schutz durch den vierten Verfassungszusatz aus.[344]

341 Katz v. United States, 389 U. S. 347 (361).
342 United States v. Miller, 425 U. S. 435 (*bank records*); Smith v. Maryland, 442 U. S. 735 (*phone numbers*).
343 Hoffa v. United States, 385 U. S. 293.
344 Harris v. United States, 390 U. S. 234.

4. *Special Needs Doctrine* – Unter bestimmten Umständen, nämlich in der Regel bei Durchsuchungen durch Staatsbeamte (z. B. Schulbeamte, Regierungsangestellte), die keine Strafverfolgungsbehörden sind, kann eine Durchsuchung nur *reasonable* sein.[345]

Der Supreme Court hat im Rahmen der objektiven Prüfung der begründeten Erwartung auf *privacy* die *Third-Party-Doctrine* angewendet, nach der die mit Dritten – wie Banken, Telefongesellschaften, Internet-Service-Providern (ISPs) und E-Mail-Servern – geteilten Informationen nicht mehr privat sind.[346] Die *Katz*-Prüfung findet auch in dem *Smith v. Maryland*-Fall Anwendung, in dem es um die Verwendung einer Technik (*Pen Register*) geht, die von Telefongesellschaften verwendet wird, um die von einem bestimmten Telefon gewählten Telefonnummern aufzuzeichnen. Das Gericht entschied, dass *Smith* einen Teil seiner *privacy* gegenüber der Telefondienstleistung preisgegeben hat. Es führte ferner aus, dass er zugunsten eines Briefversands auf das Telefon hätte verzichten müssen, wenn er seine Kommunikation hätte vollständig privat halten wollen.[347] Da es keine Möglichkeit gibt, die gewählten Telefonnummern selbstständig zu verschleiern und er sie mit Dritten geteilt hat, bestehe keine unbegründete Durchsuchung.[348] Hiernach zog der Supreme Court beim *Ciaolo*-Fall mit Hilfe der *Katz*-Prüfung den Schluss, dass einerseits alles, was von jedem wahrgenommen werden kann, mit der Öffentlichkeit geteilt wird und somit nicht privat sein könne und dass andererseits der Bau eines Zauns nicht genug sei, um eine Erwartung auf *privacy* zu schaffen.[349] Demzufolge wurde die begründete Erwartung auf *privacy* verneint.[350] Bei Müllsäcken, die am Straßenrand für die Abholung abgestellt wurden, wird die Erwartung auf *privacy* zwar festgestellt, sie ist jedoch unbegründet.[351] Denn laut

345 O'Connor v. Ortega, 480 U. S. 709.
346 Smith v. Maryland, 442 U. S. 735 (749).
347 Smith v. Maryland, 442 U. S. 735 (742).
348 Smith v. Maryland, 442 U. S. 735 (749): In einer abweichenden Meinung äußerte der Richter *Marshall* seine Ablehnung der bestehenden *Third-Party-Doctrine* des Gerichtshofs. Nach seiner Auffassung kann man seine Informationen mit einer, deshalb aber nicht notwendigerweise auch mit anderen Parteien teilen wollen.
349 California v. Ciaolo, 476 U. S. 207 (213).
350 California v. Ciaolo, 476 U. S. 207: Das Gericht begründet, dass etwas außerhalb der Wohnung, das von einem öffentlichen Raum mit dem bloßen Auge gesehen werden kann, nicht als private Information in Betracht kommt. Das Gericht behandelt leider nicht das Problem der technischen Maßnahme der polizeilichen Nutzung von *aircraft*.
351 California v. Greenwood, 486 U. S. 35 (40).

der *Third-Party-Doctrine* sind die Müllsäcke zum Zwecke der Abholung im Rahmen der Müllabfuhr in die Öffentlichkeit gestellt worden.[352]

Der technische Fortschritt führt wiederum zu einer wichtigen Änderung der *Katz*-Prüfung. Er macht es erforderlich, die Bedeutung des Ausdrucks der begründeten Erwartung auf *privacy* und des physischen Raums beim Schutz der *privacy* wieder abzuschwächen. Bezüglich des Einsatzes von Wärmebildkameras[353] wurde z. B. die Frage gestellt, ob der Einzelne eine bestimmte Tätigkeit ausüben kann, die eine Erwartung auf *privacy* schafft, auch wenn er die neuartige Überwachungstechnologie nicht kennt. Daraufhin hat der Supreme Court ein weiteres Kriterium vorgelegt: die Gewöhnlichkeit einer eingesetzten Technologie im Hinblick auf *personal agency*. Werden der Allgemeinheit unbekannte Geräte genutzt, um den verfassungsrechtlich geschützten Raum ohne physisches Betreten zu durchsuchen, macht die Nutzung dieser Geräte zu Zwecken einer Durchsuchung im Sinne des vierten Verfassungszusatzes eine gerichtliche Anordnung erforderlich. Das Gericht hebt hervor, dass im Kontext des vierten Verfassungszusatzes nicht die Fläche eines Raums geschützt wird, sondern eine staatliche Kenntnisnahme von etwas, was im Raum geschieht. Das Recht auf *privacy* sei eher das Recht, eine staatliche Kenntnisnahme zu verhindern, als das Recht, staatliches Eindringen ohne den *due process* zu vermeiden.[354]

Zusammenfassend lässt sich feststellen, dass ein privater Lebensraum verfassungsrechtlich zunächst gegen das physische Betreten des Raums durch staatliche Organe im Kontext des vierten Verfassungszusatzes geschützt wird. Dieser Schutz des Rechts auf *privacy* wurde durch die *Katz*-Prüfung erweitert und hängt nunmehr nicht ausschließlich von der räumlichen Sicht ab, sondern wird über die subjektive und die objektive Prüfung des Rechts festgelegt. Dies bedeutet, dass sich das Recht auf *privacy* vom Schutz eines Raums als solchem hin zum Schutz vor der staatlichen Kenntnisnahme von etwas, was im Raum geschieht, ändert. Außerdem wendet der Supreme Court nach der *Katz*-Entscheidung die *Third-Party-Doctrine* an, nach der die mit Dritten geteilten Informationen nicht mehr als privat angesehen werden. Darüber hinaus wurde mit der Rechtsprechung die Möglichkeit dafür eröffnet, den verfassungsrechtlich geschützten Raum gegen technikgestützte Maßnahmen zu sichern, wenn

352 California v. Greenwood, 486 U. S. 35 (40).
353 Kyllo v. United States, 533 U. S. 27.
354 Kyllo v. United States, 533 U. S. 27 (35 f.).

dieser Schutz außerdem noch davon abhängt, ob man sich an die eingesetzten technischen Mittel gewöhnt.

2. Die Bedeutung des Datenschutzes für die Privacy Protection

Das Datenschutzrecht und das allgemeine Persönlichkeitsrecht als Ursprung für das Datenschutzrecht firmieren weitestgehend gemeinsam unter dem allgemeinen *Privacy*-Begriff. Da es in den USA außerdem an verfassungsrechtlich ausdrücklichen, datenschützenden Regelungen mangelt, ist es erforderlich, das wenig ausdifferenzierte Recht auf *privacy* im Hinblick auf den Datenschutz zu untersuchen. Dabei erscheint es sinnvoll, den weiten Begriff der *privacy protection* auf eine Unterkategorie des Datenschutzes zu reduzieren und diesen zu untersuchen.

Nach zahlreichen Versuchen, den Begriff der *privacy* zu definieren, konnten die informationelle Privatheit, die Privatheit der Kommunikation und die körperliche Privatheit als Hauptelemente dieses Begriffs herausgefiltert werden.[355] Mit der Zeit begannen die Gerichte, sich neben dem verfassungsrechtlichen Privatsphärenschutz im Allgemeinen auch mit dem Recht auf informationelle Privatsphäre im Besonderen zu befassen.

Im Folgenden soll daher erörtert werden, ob und gegebenenfalls wie das Recht auf die informationelle Privatheit, nämlich die *privacy* im engeren Sinne im verfassungsrechtlichen Kontext – im Rahmen des Gesetzes- und Fallrechts zur vollständigen und ganzheitlichen Rechtsvergleichung[356] – geschützt wird.

3. Der verfassungsrechtliche Datenschutz

Der verfassungsrechtliche Schutz personenbezogener Daten, sprich der *privacy* im engeren Sinne, wird nach der *Katz*-Entscheidung mit dem Prüfungskriterium „begründete Erwartung auf *privacy*" in der Rechtsprechung diskutiert und entwickelt. In der *NAACP v. Alabama*-Entscheidung[357] er-

355 *Genz*, Datenschutz in Europa und den USA, S. 41.

356 Denn das US-amerikanische Rechtssystem basiert auf unterschiedlichen Rechtsquellen und der *Doktrin* des amerikanischen Richterrechts. Das sog. *common law* spielt dabei eine bedeutende Rolle. Daher könnte eine Nachforschung und Analyse von Rechtsprechungsveränderungen im Hinblick auf den Privatsphären- und Datenschutz von großer Bedeutung sein.

357 NAACP v. Alabama, 357 U. S. 449.

fuhr ein spezifischer Bereich der Datenverarbeitung einen frühen verfassungsrechtlichen Schutz.[358] Hier hat der Supreme Court positiv das Recht politischer Gruppen festgestellt, ihre Mitgliederlisten vor staatlichen Stellen geheim zu halten. Erst im Jahr 1976 beschäftigte sich der Supreme Court zum ersten Mal mit dem Schutz personenbezogener Daten als solcher.[359] Hierbei ging es darum, dass von der Polizei an mehr als 800 Einzelhändler Flyer verteilt wurden, auf denen der Name und das Foto einer Person zu sehen waren, die verhaftet, jedoch noch nicht für schuldig erklärt worden war. Der Supreme Court stellte in dieser Entscheidung fest, dass die verfassungsrechtlichen Grundsätze der *privacy* die Datenverbreitung mittels des amtlichen Handelns der Strafverfolgungsbehörden nicht eingrenzen. Das Gericht verneinte hierbei demnach, dass diese Daten eng mit der Persönlichkeit des Einzelnen zusammenhängen. Gemäß der Entscheidung seien die in Frage kommenden Informationen lediglich beschämender Natur, sodass der *due process* im Kontext des vierten Verfassungszusatzes nicht gefordert werde. Jedoch wurden unter dem Verweis auf die *Roe v. Wade*-Entscheidung[360] Leitlinien in Bezug darauf vorgelegt, welche Art von Informationen verfassungsrechtlich geschützt werden soll. Die Leitlinien lauten wie folgt:

1. Der Einzelne hat das Recht, die Offenlegung von persönlichen Angelegenheiten durch staatliche Behörden zu vermeiden.
2. Mit diesem Recht ist auf Seiten des Staates die Pflicht verbunden, die Informationen zu schützen, zu deren Preisgabe dieser den Einzelnen zwingt.
3. Die Informationen, die eng mit den *fundamental areas* verbunden sind, werden durch das Selbstbestimmungsrecht geschützt und rechtfertigen einen stärkeren Schutz des verfassungsrechtlichen Rechts auf informationelle Privatheit.

358 *Genz*, Datenschutz in Europa und den USA, S. 46.

359 Paul v. Davis, 424 U. S. 693.

360 Roe v. Wade, 410 U. S. 113: Das Gericht wies darauf hin, „dass sich die persönlichen Rechte in dieser Garantie der *privacy* darauf beschränken sollen, was fundamental oder implizit im Konzept der geordneten Freiheit sei". Nach der *Paul*-Entscheidung seien die detaillierten Aktivitäten, die unter diese Definition fallen, Angelegenheiten, die mit Ehe, Zeugung, Schwangerschaftsverhütung, Familienbeziehungen und Kindererziehung sowie -bildung im Zusammenhang stehen (Paul v. Davis, 424 U. S. 693 (713)).

Ein Jahr nach der *Paul v. Davis*-Entscheidung stellte der Supreme Court in seiner *Whalen v. Roe*-Entscheidung[361] fest, dass unter dem Recht, in Ruhe gelassen zu werden, das individuelle Interesse an einer Vermeidung der Offenlegung persönlicher Angelegenheiten zu verstehen sei. Im Rahmen dieser Feststellung erkannte der Supreme Court das Recht auf die informationelle Privatheit und den verfassungsrechtlichen Freiheitsschutz an. Die Verfassung erkenne demnach ein berechtigtes Interesse der *privacy* an sensiblen persönlichen Informationen an. Der Fall wurde vom Gericht verhandelt, damit die Verfassungskonformität des Landesgesetzes in New York überprüft werden kann. Nach dem Gesetz sollten die Rezepte eingebracht werden, in denen bestimmte von der Landesregierung als gefährlich eingeordnete Arzneimittel gelistet sind. Das Amtsgericht hatte festgestellt, dass das Gesetz unnötig in die Arzt-Patient-Beziehung eingreife, die als eine der verfassungsrechtlich schutzwürdigsten Zonen der *privacy* gilt.[362] Hierbei unterschied der Supreme Court zunächst zwischen Vertraulichkeits- und Selbstbestimmungsinteressen im Rahmen des Rechts auf informationelle Privatheit und entschied dann, dass das direkte Eingreifen des Landes New York in die Arzt-Patient-Beziehung keine Gefährdung des Selbstbestimmungsinteresses sei, da der Zugang zu Medikamenten nicht von der Zustimmung eines staatlichen Beamten oder sonstiger Dritter abhängt.[363] Eine Gefährdung der Vertraulichkeit wurde hingegen vom Gericht akzeptiert. Um solche Herausforderungen im Rahmen des Rechts auf informationelle Privatheit zu überwinden, wandte das Gericht einen Abwägungsansatz an.[364] Der Abwägung zwischen dem öffentlichen Interesse am Zugriff auf die personenbezogenen Daten als einem Teil der *privacy* und dem gefährdeten individuellen Interesse wurde eine Begleitungspflicht des Staates als eine neue Variable hinzugefügt.[365] Der Supreme Court erkannte hierbei zwar an, dass im *Privacy*-Schutz zwei unterschiedliche Interessen enthalten sind, nämlich zum einen das Interesse des Einzelnen an der Vermeidung der Bekanntmachung seiner persönlichen Angele-

361 Whalen v. Roe, 429 U. S. 589.
362 Roe v. Ingraham, 403 F. Supp. 931 (D. C. N. Y. 1975).
363 Whalen v. Roe, 429 U. S. 589 (598 f. und 602, 603).
364 Der Ansatz wurde seit der *Griswold v. Connecticut*-Entscheidung im Autonomie-Zweig der Privatsphäre verwendet, damit die Verfassungsmäßigkeit von Gesetzen entschieden wird, die eine selbstbestimmte Entscheidung verhindern.
365 Der Richter Stevens behauptet, „die Befugnis, Daten für die öffentlichen Zwecke zu sammeln und zu nutzen, ist in der Regel von einer gleichzeitigen gesetzlichen oder behördlichen Pflicht zur Vermeidung von unberechtigten Angaben begleitet" (Whalen v. Roe, 429 U. S. 589 (605)).

genheiten und zum anderen das Interesse an der Selbstbestimmung bei wichtigen Entscheidungen; das Gericht entschied jedoch, dass bei diesem Fall keine unbegründete Verletzung der beiden Interessen vorliegt. Denn soweit die Sicherheitsverfahren nach dem Gesetz eingehalten werden, sei die Möglichkeit der Bekanntmachung der gespeicherten Daten relativ gering. Auch die Ablehnung des Eingriffs in das Selbstbestimmungsrecht sei auf die Statistik über die Anzahl der ausgestellten Rezepte nach dem Inkrafttreten des Gesetzes gestützt.[366]

Kurz nach der *Whalen*-Entscheidung verfocht der frühere Präsident *Nixon* die Verfassungsverletzung des Presidential Recordings and Materials Preservation Act in der *Nixon*-Entscheidung. Nach dem Gesetz sollte die GSA (*General Services Administration*) alle Dokumente und Tonbänder während seiner Amtszeit als Präsident speichern. Der Kläger behauptete deshalb die Verletzung des Rechts auf *privacy*, da ein Teil der eingezogenen Dokumente sowie Tonbänder private Unterlagen darstelle, die das Amt keineswegs betreffen. Der Richter *Brennan* stellte fest, dass auch der frühere Präsident das verfassungsrechtliche Recht auf seine *privacy* beanspruchen konnte[367] und er eine legitime Erwartung auf *privacy* hatte.[368] Der Abwägungsansatz führte zu keiner Verletzung des Rechts auf Geheimhaltung der persönlichen Angelegenheiten, da das hier involvierte archivische Überprüfungsverfahren eher dem „wichtigen öffentlichen Interesse" und dem „wichtigen Staatsinteresse" und weniger dem Privatheitsinteresse diente.[369] Entsprechend der *Whalen*-Entscheidung sieht der Supreme Court das Interesse des Einzelnen an der Vermeidung der Bekanntmachung persönlicher Angelegenheiten als einen Teil der *privacy*. Das Interesse des Einzelnen habe bei diesem Fall einer Abwägung gegen das öffentliche Interesse an der Unterwerfung der präsidentiellen Materialien unter die archivalische Überprüfung bedurft. Der Gerichtshof ent-

366 Whalen v. Roe, 429 U. S. 589 (599 ff.).
367 Nixon v. Administrator of General Services, 433 U. S. 425 (457).
368 Nixon v. Administrator of General Services, 433 U. S. 425 (465).
369 Nixon v. Administrator of General Services, 433 U. S. 425 (464 ff.).

schied unter Berücksichtigung der gesetzlichen Sicherungsmaßnahme im Gesetz,[370] dass das öffentliche Interesse überwiege.[371]

Nach den Bewertungen der Circuit Courts hat der Supreme Court zwar deutlich gemacht, dass das Interesse des Einzelnen an der Vermeidung der Offenlegung persönlicher Angelegenheiten zum einen und zum anderen das Interesse an der Selbstbestimmung bei bedeutungstragenden Entscheidungen in der Verfassung wurzeln, er hat jedoch keine nachvollziehbaren Leitlinien vorgelegt, die bei Überprüfungen der mit der informationellen Privatheit in Zusammenhang stehenden Fälle anwendbar sind.[372] Die nachvollziehbaren Leitlinien werden eher von den Circuit Courts entwickelt. Wie der Supreme Court prüfen auch sie die Verfassungskonformität im Rahmen eines Eingriffs in persönliche Daten als solche mit Hilfe des Abwägungsansatzes.[373] Mit dem äußerst vagen Wegweiser des Supreme Court haben die Circuit Courts eine nützliche Abwägungsgleichung entwickelt, mit der Fälle lösbar sind, die die informationelle Privatheit betreffen. Werden ihre Entscheidungen zusammengefasst, kann die ähnlich angewandte Abwägungsgleichung so formuliert werden:[374]

> Individuelles Privatsphäreninteresse = (Informationstyp – Klägerkategorie) – staatliche Sicherungsmaßnahme

---

370 Siehe Nixon v. Administrator of General Services, 433 U. S. 425 (458 ff.): Der Richter *Brennan* erklärt, dass das Gesetz nicht nur Maßnahmen vorsieht, die darin bestehen, die übermäßige Verbreitung von privaten Materialien zu verhindern, sondern dass der Staat im Gegensatz zum *Whalen*-Fall eine langfristige Kontrolle über solche privaten Informationen nicht einmal behalten wird.

371 Bei einer abweichenden Meinung behauptet der Präsident des Supreme Court *Burger*, dass das öffentliche Interesse, das die Regierung genannt hat, aus Mangel an konkreten Zielsetzungen nicht mehr als ein generalisierter Bedarf sei und demnach das Interesse des Präsidenten an seiner Privatsphäre überwiege (Nixon v. Administrator of General Services, 433 U. S. 425 (528 ff.)).

372 So alle Circuit Courts außer dem 6. Circuit Court. Vgl. Barry v. City of New York, 712 F. 2d. 1554 (1559) (2nd Cir. 1983): Obwohl der Supreme Court anerkannte, dass das Recht des Einzelnen auf das Vermeiden der Bekanntmachung persönlicher Angelegenheiten seine Wurzeln in der Verfassung hat, bedauert der Richter *Wilfred Feinberg*, dass das Wesen und der Umfang des Interesses sowie die entsprechenden Prüfungsmaßstäbe für angebliche Verletzungen dieses Interesses nach wie vor unklar sind.

373 Vgl. Plante v. Gonzales, 575 F. 2d. 1119 (5th Cir. 1978); Fadjo v. Coon, 633 F. 2d. 1172 (5th Cir. 1981); Barry v. City of New York, 712 F. 2d. 1554 (1559) (2nd Cir. 1983); Tavoulareas v. Washington Post, 724 F. 2d. 1010 (D. C. Cir. 1984).

374 *Kuhn*, Federal Dataveillance: Implications for Constitutional Privacy Protections, S. 130.

Individuelles Privatsphäreninteresse (>, <) staatliches Interesse an Informationen = Entscheidung

Auf den jeweiligen Informationstyp wird der Grundsatz angewendet, dass umso mehr Schutz gewährt wird, je enger die Informationen mit dem fundamentalen Interesse und mit dem Selbstbestimmungsrecht verbunden sind. Die Informationen, die der Staat nach einer Verabredung der Vertraulichkeit erhebt und sammelt – unabhängig davon, ob die Vertraulichkeit durch eine ausdrückliche Verabredung oder durch ein Gerichtsverfahren gesichert ist –, genießen meist hochgradigen Schutz.[375] Daneben sind die sexuelle Orientierung[376] und das Selbstbestimmungsrecht in Ehebeziehungen[377] oder homosexuellen Partnerschaften[378] dazu geeignet, höchsten Schutz zu gewähren. Medizinische Informationen werden hingegen unterschiedlich behandelt. Informationen, die z. B. mit einem Schwangerschaftsstatus[379] oder dem HIV-Status[380] im Zusammenhang stehen, werden als intime Informationen angesehen; der Schutz für die übrigen allgemeinen medizinischen Informationen wird dagegen abgelehnt, etwa wie die vom Gericht bestellte psychiatrische Beurteilung.[381] Die Circuit Courts gewähren den finanziellen Informationen einen mittelgradigen Schutz, da diese nicht eng genug mit fundamentalen familiären Interessen im Zusammenhang stünden.[382] Nach der *Paul*-Entscheidung wird der Einzelne nicht gegen die Offenlegung persönlicher Daten geschützt, wenn diese lediglich

375 S. Fadjo v. Coon, 633 F. 2d. 1172 (5th Cir. 1981); Tavoulareas v. Washington Post, 724 F. 2d. 1010 (D. C. Cir. 1984); James. v. City Douglas, 941 F. 2d. 1539 (11th Cir. 1991).

376 Sterling v. Borough of Minersville, 232 F. 3d. 190 (3rd Cir. 2000): In diesem Fall hatte sich ein Teenager umgebracht, nachdem die regionale Polizei ihm damit gedroht hatte, seinen Großeltern zu verraten, dass er homosexuell ist. Das Gericht stellte fest, dass selbst die einfache Bedrohung einen Verstoß gegen das Recht auf Privatsphäre darstellt („the essence of the right to privacy is in avoiding disclosure of personal matters", S. 197).

377 Griswold v. Connecticut, 381 U. S. 479.

378 Eisenstadt v. Baird, 405 U. S. 438.

379 Gruenke v. Seip, 225 F. 3d. 290 (3rd Cir. 2000).

380 Herring v. Keenan, 218 F. 3d. 1171 (10th Cir. 2000).

381 Borucki v. Ryan, 827 F. 2d. 836 (842) (1st Cir. 1987): Die Entscheidung beruht darauf, dass die Inhalte dieser Berichte keine intime Informationen darstellen: „the contents of such reports did not rise to the level of the more intimate information indicated in Paul and nor did the justification for protecting such a privacy interest reside in the penumbra of any specific amendment mentioned in Griswold."

382 Vgl. Plante v. Gonzales, 575 F. 2d. 1119 (5th Cir. 1978); Barry v. City of New York, 712 F. 2d. 1554 (2nd Cir. 1983).

beschämender Natur sind.[383] Außerdem genießt das *Privacy*-Interesse an persönlichen Daten beim öffentlichen Eintrag, z. B. beim Verhaftungsdaten, den niedrigsten Schutz.[384] Der vierte Verfassungszusatz wurde sowohl auf personenbezogene Daten unter der Herrschaft Dritter als auch auf sog. Daten ohne Inhaltwie beispielsweise Telefonnummern als unanwendbar angesehen.[385]

Im Rahmen der sog. Klägerkategorie wird geprüft, ob eine bestimmte Qualität das individuelle Interesse schwächt, beispielsweise die mit Steuergeld verdiente[386] oder die ein öffentliches Vertrauen erfordernde Stellung[387] oder die Stellung als Gefangener.[388]

Bei einer staatlichen Sicherungsmaßnahme wird danach gefragt, ob (und wie) der Staat seine Pflicht erfüllt, die von ihm bestellten Informationen zu schützen. Je ausgeprägter die staatlichen Garantien in den Augen des Gerichts erscheinen, desto geringer ist das wahrgenommene Risiko. Das Gericht stellte fest, dass z. B. in der *Barry*-Entscheidung die Sicherungsmaßnahme bereits ausreichend sei, da das gesetzliche Verfahren den Mitarbeitern der Stadt eine Klagemöglichkeit eröffne, um bestimmte Typen von Informationen gegen die Offenlegung vor der Öffentlichkeit zu schützen.[389] Darüber hinaus sei der *coding process* für die erforderlichen Sicherungsmaßnahmen geeignet, um die Informationen von Patienten zu schützen.[390]

Das staatliche Interesse an Informationen als das letzte Element der Abwägungsgleichung teilt sich grob in drei Stufen: das berechtigte, das wesentliche und das zwingende Interesse. Ein berechtigtes Interesse kann die Prüfung bestehen und ein wesentliches Interesse wird unter der intermediären Prüfung gewährleistet, während ein zwingendes Interesse einer strikten Prüfung unterzogen werden soll. Je enger eine bestimmte Information mit fundamentalen Werten verbunden ist, desto zwingender

383 Siehe Alexander v. Peffer, 993 F. 2d. 1348 (8th Cir. 1993).
384 Siehe Eagle v. Morgan, 88 F. 3d. 620 (8th Cir. 1996); Russell v. Gregoire, 124 F. 3d. 1079 (1094) (9th Cir. 1997).
385 *Schwartz*, Zur Architektonik des Datenschutzes in den USA, in: *Stern/Pfeifer/Hain*, Datenschutz im digitalen Zeitalte, S. 113 f.
386 Vgl. Barry v. City of New York, 712 F. 2d. 1554 (2nd Cir. 1983); Plante v. Gonzales, 575 F. 2d. 1119 (5th Cir. 1978).
387 Vgl. Nat. Fed'n of Fed. Employers v. Greenberg, 983 F. 2d. 286 (D.C. Cir. 1993).
388 Vgl. Eagle v. Morgan, 88 F. 3d. 620 (8th Cir. 1996); Russell v. Gregoire, 124 F. 3d. 1079 (1094) (9th Cir. 1997).
389 Barry v. City of New York, 712 F. 2d. 1554 (1561 ff.) (2nd Cir. 1983).
390 Schacter v. Whalen, 581 F. 2d. 35 (37) (2nd Cir. 1978).

soll das staatliche Interesse sein, um einen Verstoß gegen das Recht auf informationelle Privatsphäre zu rechtfertigen. Die Circuit Courts erklären das staatliche Interesse an der Verbesserung des Wahlprozesses mit der Begründung für wesentlich, dass durch die Transparenz bei den Wählern das Vertrauen erhöht wird.[391] Die Förderung der öffentlichen Sicherheit und Wohlfahrt wird ebenfalls als ein wesentliches Interesse angesehen.[392] Der Staat verliert dann einen Prozess, wenn kein staatliches Interesse vorhanden ist.[393]

Nach fortdauernden Entscheidungen der Circuit Courts wurde dem Supreme Court erst wieder im Jahr 2011 ein Anlass gegeben, um eine endgültige Entscheidung über die Verletzung des Rechts auf informationelle Privatheit zu treffen. In diesem Fall ging es darum, ob die Hintergrundüberprüfung des Vertragspersonals durch die NASA das Recht auf die informationelle Privatheit verletzte.

Entsprechend der leitenden Weisung des damaligen Präsidenten *George W. Bush*, die neuen gleichförmigen Identifizierungsstandards für das Bundespersonal einschließlich des Vertragspersonals zu gestalten, ordnete das Handelsministerium an, dass das Vertragspersonal, das schon lange Zugang zu Bundeseinrichtungen hatte, bis zum Oktober 2007 die Hintergrundüberprüfung vollenden musste. Das *Jet Propulsion Laboratory (JPL)* ist eine Einrichtung der NASA, die das *California Institute of Technology (Caltech)* unter staatlichem Vertrag führt. Im Januar 2007 änderte die NASA den mit Caltech abgeschlossenen Vertrag. Nach dem neuen Vertrag musste das gesamte Personal des JPL die neue Hintergrundüberprüfung rechtzeitig ausführen.

Aus diesem Grund erhoben die Beklagten eine Klage unter Berufung darauf, dass das Hintergrundüberprüfungsverfahren das verfassungsrechtli-

391 Plante v. Gonzales, 575 F. 2d. 1119 (5th Cir. 1978): Floridas *Sunshine Amendments* liefern den Wählern mehr Informationen über Kandidaten und die finanziellen Offenlegungsvorschriften zielen darauf ab, die Wahrscheinlichkeit von Korruption oder Interessenkonflikten zu verringern (1134 ff.). Obwohl der Richter *Wisdom* Zweifel an der Effektivität der Amendments zur Abschreckung vor Korruption gezeigt hat, erkannte er die potenzielle Effektivität an und erklärte die Amendments für legitim. Für eine ähnliche Begründung siehe auch Barry v. City of New York, 712 F. 2d. 1554 (1560 ff.) (2nd Cir. 1983).

392 Schacter v. Whalen, 581 F. 2d. 35 (37) (2nd Cir. 1978); Zum Schutz der Gesundheit und Sicherheit von Arbeitskräften, S. Westinghouse, 638 F. 2d. 570 (579) (3rd. Cir. 1980).

393 Vgl. Fadjo v. Coon, 633 F. 2d. 1172 (5th Cir. 1981); Tavoulareas v. Washington Post, 724 F. 2d. 1010 (D. C. Cir. 1984); James. v. City Douglas, 941 F. 2d. 1539 (11th Cir. 1991); Gruenke v. Seip, 225 F. 3d. 290 (3rd Cir. 2000).

che Recht auf die informationelle Privatheit verletzt. Während das Amtsgericht eine einstweilige Verfügung leugnete, wies das *Ninth Circuit Court* die Anordnung des Amtsgerichts ab. Es entschied, dass einige Teile des Formulars zur Hintergrundüberprüfung wahrscheinlich verfassungswidrig sind, z. B. die Bekanntgabe von Drogenbehandlungen oder Beratungen u. a. Die Regierung beantragte daher eine Revision.

Die Grundannahme des Supreme Court vor der konkreten Überprüfung lautet, dass die Verfassung das Recht auf die informationelle Privatheit schütze, das in beiden oben genannten Entscheidungen, *Whalen* und *Nixon*, erwähnt wurde.[394] Der Supreme Court entschied danach, dass die Hintergrundüberprüfung der NASA ein solches Recht nicht verletzt habe. Der Schutz der *privacy* umfasse gemäß dem Supreme Court tatsächlich mindestens zwei unterschiedliche Arten des Interesses: zum einen das Interesse an der Vermeidung der Offenlegung persönlicher Angelegenheiten, zum anderen das Interesse an der Selbstbestimmung ohne staatliche Intervention.[395] Die Regierung habe ein Interesse an der Durchsetzung der Hintergrundüberprüfung zur begründeten Einstellung und dieses Interesse hänge nicht von der Stellung als Bundespersonal oder Vertragspersonal ab. Die Erhebung persönlicher Daten durch den Staat zu öffentlichen Zwecken könne das Problem der Bedrohung der Privatsphäre verursachen. Das Problem sollte durch eine gesetzliche oder behördliche Verpflichtung gelöst werden, um die unbefugte Veröffentlichung zu vermeiden.[396] Dabei wird die Frage, ob das Recht in der amerikanischen Verfassung existiert, offengelassen. Die Richterin *Scalia* stimmt dieser Auffassung, nach der die Hintergrundüberprüfung kein bestimmtes verfassungsrechtliches Recht verletzt, zwar zu, sie behauptet jedoch, dass der Gerichtshof die Frage des verfassungsrechtlichen Rechts auf informationelle Privatheit negativ hätte lösen müssen.[397]

---

394 NASA v. Nelson, 131 S. Ct. 746 (753 f.); *Fan*, Constitutionalizing Informational Privacy by Assumption, 14 U. Pa. J. Const. L. 953, 2012 (954); *Olivito*, Beyond the Fourth Amendment: Limiting Drone Surveillance Through the Constitutional Right to Informational Privacy, Ohio State Law Journal, vol. 74, no. 4 669, 2013 (689 f.); *Moniodis*, Moving from Nixon to NASA: Privacy's Second Strand – A Right to Informational Privacy, 15 YALE J. L. & Tech. 139, 2012 (148).

395 Whalen v. Roe, 429 U. S. 589 (599); NASA v. Nelson, 131 S. Ct. 746 (753); *Azarchs*, Informational Privacy: Lessons from Across the Atlantic, 16 U. Pa. J. Const. L. 805, 2014 (807).

396 NASA v. Nelson, 131 S. Ct. 746 (753); Whalen v. Roe 429 U. S. 589 (600 f.).

397 Sie verneint bei der Zustimmungsmeinung das Konzept des verfassungsrechtlichen Rechts auf die informationelle Privatsphäre. Ihre Ansicht stützt auch der

Daher lässt sich feststellen, dass der Supreme Court den verfassungsrechtlichen Schutz des Rechts auf informationelle Privatheit nur vermutet und entsprechend der *Whalen*- und der *Nixon*-Entscheidung das Recht in zwei Teile differenziert, und dass auch die staatliche Pflicht, die vom Staat erhobenen Informationen zu schützen, in Betracht gezogen wurde. Es ist jedoch unklar, ob die von Circuit Courts entwickelte konkrete Abwägungsgleichung vom Supreme Court bei der Abwägung beider kollidierender Interessen verwendet wurde. Nach der Abwägungsgleichung der Circuit Courts wird das Schutzniveau zuerst danach festgelegt, wie privat oder intim eine bestimmte Information ihrem Wesen nach ist. Unter Berücksichtigung des Klägerelements, das den Schutz verringert, wird der Umfang des Rechts auf informationelle Privatheit wiederum gemäß dem Kriterium festgelegt, ob eine gesetzliche oder prozedurale Sicherungsmaßnahme vorgesehen ist. Ist das individuelle Interesse einmal auf diese Weise festgesetzt, kann die Verletzung der angegriffenen Vorschriften oder des staatlichen Handelns mit Hilfe der Abwägung geprüft werden. Das Gericht gewährt in der Regel den höchsten Schutz für die Informationen, die den Autonomiebereich berühren oder die medizinische Informationen von intimem Charakter (z. B. Schwangerschafts- oder HIV-Status) darstellen, während, relativ gesehen, allgemeine medizinische, finanzielle oder beschämende Informationen aufgrund der Tatsache, dass es sich bei ihnen nicht um höchstpersönliche Informationen handelt, weniger geschützt werden. Die staatliche Pflicht zum Vertraulichkeitsschutz wird konkret, aber gegebenenfalls vordergründig bewertet.

Es lässt sich folgern, dass die persönlichen Daten als solche durch den Staat unterschiedlich, nämlich je nach Art ihrer Sensibilität, dann erhoben und verwertet werden dürfen, wenn die Sicherungsmaßnahmen vorgesehen sind – wobei es keine Rolle spielt, ob sie hinreichend sind, um die personenbezogenen Daten vor der unbefugten Erhebung oder Verwertung zu schützen – und wenn das staatliche Handeln der Abwägungsprüfung standhalten kann. Umgekehrt wird die staatliche Erhebung und Verwertung von persönlichen Daten, die der Abwägungsprüfung nicht standhalten, als eine Verletzung des Rechts auf *privacy* angesehen.

Richter Thomas mit seiner kurzen zustimmenden Stellungnahme. (NASA v. Nelson, 131 S. Ct. 746 (757)); *Azarchs*, Informational Privacy: Lessons from Across the Atlantic, 16 U. Pa. J. Const. L. 805, 2014 (806): „Ohne eine klare Textgrundlage haben die Gerichte wenig Befugnis, ein solches Recht zu verteidigen, wenn es von den beiden anderen Regierungszweigen verletzt wird, und wenig Richtlinien zur Festlegung seiner Grenzen".

Obwohl der Supreme Court das Recht auf informationelle Privatheit nicht ausdrücklich feststellt, sondern nur implizit von dessen Existenz ausgeht, garantiert die US-amerikanische Verfassung für einen engen, inneren und speziellen Bereich den Schutz der *privacy* zumindest vor hoheitlichen Eingriffen. Es ist bemerkenswert, dass der Schutz der *privacy* mit Hilfe des Kriteriums „begründeter Erwartung auf *privacy*" erweitert wird und dass das Recht auf informationelle Privatheit unter der Differenzierung zwischen dem Vertraulichkeitsinteresse und dem Autonomieinteresse diskutiert wird. Bezüglich der Frage nach dem Schutz des Rechts auf informationelle Privatheit liegt die erhebliche Schwäche darin, dass das Gericht lediglich vor der Offenlegung Schutz gewährt, nicht aber bezüglich aller Verarbeitungsvorgänge von personenbezogenen Daten wie deren unbefugter Erhebung, Speicherung, interner Übermittlung innerhalb der öffentlichen Stellen sowie deren Verwertung.

Angesichts des Umstands, dass es nach US-amerikanischer Dogmatik keine Idee von einer Schutzpflicht des Staates gibt, aktive Maßnahmen zum Schutz der *privacy* von Individuen zu ergreifen, und daher die aus der US-Verfassung ableitbaren Rechte ausschließlich als Abwehrrechte gegenüber dem Staat zu verstehen sind, erscheint der Datenschutz durch ein generelles und fundamentales Recht auf informationelle Selbstbestimmung als sehr unwahrscheinlich.

II. Übersicht des einfachgesetzlichen Datenschutzsystems

Auch wenn die personenbezogenen Daten verfassungsrechtlich nicht ausdrücklich geschützt werden können, kann das Bundesgesetz Schutzmaßnahmen vorschreiben und dem Staat, der die Informationen anfordert, Prozessanforderungen auferlegen. Das US-amerikanische Recht kennt kein allgemeines Datenschutzrecht, welches die Privatsphäre eines Einzelnen und seine personenbezogenen Daten umfassend schützt und für alle staatlichen Organe Geltung hat. Beim Datenschutz wird in den USA ein bereichsspezifischer Regelungsansatz gewählt. Damit ist grundsätzlich jeder Datenverarbeitungsvorgang zulässig, soweit gesetzlich nichts anderes bestimmt ist. Da in vielen Einzelfällen politische Notwendigkeiten den Gesetzgeber zum Handeln trieben, konnte daraus nur eine bereichsspezifische Sondergesetzgebung entstehen. Dabei können grundsätzlich die folgenden Bundesgesetze gelten: 1. der Electronic Communications Privacy Act (ECPA), das aus dem Wiretap Act (18 U. S. C. §§ 2510–2522), das eine strenge Kontrolle für das „interception" der Kommunikationen

bietet, dem Stored Communications Act (18 U. S. C. §§ 2701–2711), der vorschreibt, dass die Behörden mit *subpoena*,[398] *court order* oder *warrant*[399] auf gespeicherte Daten im elektronischen Speicher zugreifen müssen und dass die Behörden *warrant* oder *court order* einholen müssen, um auf bestimmte Kundendaten von ISPs zugreifen zu können, und dem Pen Register Act (18 U. S. C. §§ 3121–3127) besteht, der vor der Installation des Pen Registers ein *court order* erfordert; 2. der Privacy Act (5 U. S. C. § 552a), der einen Code of Fair Information Practice festlegt, der die Erhebung, Verwendung und Übermittlung von personenbezogenen Daten über Personen regelt, die von Bundesbehörden geführt werden; 3. der Privacy Protection Act (PPA) (42 U. S. C. § 2000aa), der Mediendokumente und Arbeitsprodukte vor behördlichen Durchsuchungen und Beschlagnahmen schützt; 4. der Right to Financial Privacy Act (RFPA) (12 U. S. C. §§ 3401–3422), der den Kunden von Finanzinstituten das Recht auf ein gewisses Maß an *privacy* bei behördlichen Durchsuchungen gibt und verhindert, dass Banken und andere Finanzinstitute die Finanzinformationen einer Person an die Behörden weitergeben, es sei denn, die Daten werden aufgrund einer *subpoena* oder eines Durchsuchungsbefehls veröffentlicht[400] und 5. der Foreign Intelligence Surveillance Act (50 U. S. C. §§ 1801–1811), der Standards und Verfahren für die Verwendung

398 Eine *subpoena* ist eine Anordnung für eine Einholung von Zeugnissen oder Unterlagen. Zahlreiche Gesetze ermächtigen die Bundesbehörden zur Ausstellung von *subpoenas*. Die Ausstellung einer *subpoena* setzt einen „Grund zu der Annahme voraus, dass die angeforderten Daten für eine rechtmäßige Strafverfolgungsuntersuchung relevant sind." Wenn der Betroffene, der eine *subpoena* erhält, Einwände hat, kann er eine Klage einreichen, um die *subpoena* aufheben oder ändern zu lassen. Das Gericht kann die *subpoena* aufheben oder ändern, wenn ihre Einhaltung unvernünftig oder unterdrückend erscheint (Fed. R. Crim. P. 17 (c) (2)).

399 Eine *court order* und ein *warrant* unterscheiden sich durch ihre Anforderungen. Ein *warrant* wird durch einen wahrscheinlichen Grund (probable cause) gestützt, während eine *court order* konkrete und klar umrissene Tatsachen erfordert, aus denen hervorgeht, dass Grund zu der Annahme besteht, dass die gesuchten Informationen für die strafrechtliche Ermittlung relevant sind.

400 United States v. Dionisio, 410 U. S. 1: Eine *subpoena* der *Grand Jury* löst keinen Schutz des vierten Verfassungszusatzes aus; Gonzales v. Google, 234 F. R. D. 674 (N. D. Cal. 2006): Die Behörde stellte eine *subpoena* für die Suchanfragendaten von Google aus, um die Wirksamkeit der *content filtering software* zu untersuchen. Das Gericht gestattete der Behörde nicht, Informationen über Suchanfragen zu erhalten, da „der Verlust des Goodwills von Google eine potenzielle Belastung darstellt, wenn Google gezwungen ist, Suchanfragen an die Behörden weiterzuleiten".

der elektronischen Überwachung durch die Behörden zum Sammeln von Auslandsnachrichten in den USA festlegt.

Die Gesetzgebung auf Bundesebene beruht auf einer Unterstützung selbstregulativer Verfahrensweisen der US-Handelsaufsicht *FTC*. Gemäß der Rechtspolitik der Selbstregulierung ist die Regulierung wesentlicher Bereiche im gesellschaftlichen Leben den Betroffenen selbst überlassen. Der Staat fördert zwar (mehr oder minder stark) Leitlinien „guten" selbstregulativen Datenschutzes, die Form der Selbstregulierung bleibt jedoch den betroffenen gesellschaftlichen Kräften überlassen. So stützen sich die USA im Rahmen des Datenschutzes auf den Flickenteppich eng fokussierter sektoraler Gesetze und freiwilliger Selbstregulierung.[401] Die gesetzlichen spezifischen Datenschutzvorschriften in den USA können in zwei Kategorien nach Normadressaten aufgeteilt werden: zum einen Datenschutz im öffentlichen Sektor – für den Staat und seine Organe –, zum anderen Datenschutz im privaten Sektor – hinsichtlich des Schutzes Privater gegenüber Privaten.

1973 veröffentlichte das *U. S. Department of Health, Education & Welfare* (HEW) einen einflussreichen Bericht,[402] in dem eine Reihe von fair information practices (FIPs) empfohlen wurden:

1. Es darf keine Systeme zur Aufbewahrung personenbezogener Daten geben, deren Existenz geheim ist.
2. Es muss dem Einzelnen eine Möglichkeit gegeben werden, herauszufinden, welche Informationen über ihn in einem Datensatz enthalten sind und wie sie verwendet werden.
3. Es muss für den Einzelnen eine Möglichkeit bestehen, zu verhindern, dass für einen bestimmten Zweck erhaltene Informationen ohne seine Zustimmung für andere Zwecke verwendet oder zur Verfügung gestellt werden.
4. Der Einzelne muss identifizierbare Informationen über sich korrigieren oder ändern können.
5. Jede Organisation, die die Datensätze identifizierbarer personenbezogener Daten erstellt, verwaltet, verwendet oder übermittelt, muss die Zuverlässigkeit der Daten für ihren beabsichtigten Gebrauch gewähr-

401 Daneben haben die Einzelstaaten auch Gesetze, die die elektronische Überwachung und den Zugang zu Computern regeln. In einigen Staaten sehen diese Gesetze strengere Datenschutzbestimmungen vor als die Bundesgesetze.

402 *U. S. Department of Health, Education & Welfare*, Records, Computers, and the Rights of Citizens: Report of the Secretary´s Advisory Committee on Automated Personal Data Systems, 1973.

leisten und angemessene Vorkehrungen treffen, um einen Missbrauch der Daten zu verhindern.

Diese FIPs wurden in verschiedenen US-Datenschutzbestimmungen verkörpert. Aufgrund der Vielzahl von Gesetzen ist es unmöglich, sie alle übersichtlich vorzustellen. Unter diesen Gesetzen ist jedoch beispielsweise der Privacy Act[403] nennenswert. Das Gesetz legt eine Reihe von fair information practices fest, die die Erhebung, Verwaltung, Verwendung und Übermittlung personenbezogener Daten über Personen regeln, die von Bundesbehörden in Datenspeicherungssystemen geführt werden. Das Gesetz schützt als direkte gesetzgeberische Folge der sog. Watergate-Affäre die Privaten gegen hoheitliche Eingriffe in ihre Privatsphäre. Für die Daten, die von Bundesbehörden geführt werden, gelten nach dem Privacy Act folgende Grundsätze: das Übermittlungsverbot ohne Zustimmung der Betroffenen, der Zweckbindungsgrundsatz, die Datenvermeidung und -sparsamkeit, die Benachrichtigungspflicht, die Datensicherheit usw. Sein wesentlicher Grundsatz ist, die Datensammlung soweit möglich bei der betroffenen Person durchzuführen.[404] Nach diesem Gesetz darf keine Behörde Daten, die in einem Datenspeicherungssystem enthalten sind, auf beliebige Art und Weise an eine Person oder eine andere Behörde weitergeben, es sei denn, dies erfolgt auf schriftliche Anfrage oder mit vorheriger schriftlicher Zustimmung der Betroffenen.[405] Die Behörden dürfen nur jene Daten über eine Person speichern und verwalten, die relevant und notwendig sind, um einen Zweck der Behörde zu erfüllen, der gesetzlich oder auf Anordnung des Präsidenten zu erfüllen ist.[406] Eine Person muss auf Anfrage darüber benachrichtigt werden, wie ihre personenbezogenen Daten verwendet werden.[407] Die Behörden sind darüber hinaus auch dazu verpflichtet, angemessene administrative, technische und physische Schutzmaßnahmen zu treffen, um die Sicherheit und Vertraulichkeit der Daten zu gewährleisten.[408] Außerdem wird das Recht der Betroffenen auf Einsichtnahme und gegebenenfalls Berichtigung der über sie gesammelten Daten gewährleistet.[409] Der Privacy Act enthält jedoch viele Möglichkeiten bezüglich der Ausnahmen für die Daten, die nicht unter die Anforderun-

403 5 U. S. C. § 552a von 1974.
404 5 U. S. C. § 552a (e).
405 5 U. S. C. § 552a (b).
406 5 U. S. C. § 552a (e) (1).
407 5 U. S. C. § 552a (e) (3).
408 5 U. S. C. § 552a (e) (10).
409 5 U. S. C. § 552a (d).

gen des Gesetzes fallen. Diese Ausnahmen umfassen unter anderem: (1) die Daten zu Strafverfolgungszwecken; (2) die Daten, die gemäß dem FOIA offengelegt werden müssen; (3) die Daten, die für eine routine use offengelegt werden, wenn die Offenlegung mit dem Zweck vergleichbar ist, für den die Behörde diese Daten gesammelt hat; (4) die Offenlegung von Daten gegenüber dem *Census Bureau*; (5) die Offenlegung von Daten gegenüber einer Person aufgrund eines Nachweises zwingender Umstände, die sich auf ihre Gesundheit oder Sicherheit auswirken; (6) die Offenlegung gegenüber dem Kongress; (7) die Offenlegung gegenüber dem *Comptroller General*; (8) die Offenlegung aufgrund eines Gerichtsbeschlusses; (9) die Offenlegung gegenüber einer *credit reporting agency*.[410] Das Gesetz ist deshalb von Bedeutung, weil es das erste gesamtstaatliche Gesetz zum Schutz Privater gegen hoheitliche Eingriffe in deren Privatsphäre ist. Es findet allerdings nur bei Regierungsstellen der Bundesbehörden Anwendung, jedoch nicht bei Regierungsstellen in den einzelnen föderalen Staaten. Neben dem Schutz der Privatsphäre vor hoheitlichen Eingriffen dienen verschiedene Normen zum Datenschutz für den privaten Bereich, etwa der Fair Credit Reporting Act oder der Gramm-Leach-Billey-Act bei Finanzdienstleistern sowie der Electronic Communications Privacy Act oder der Children's Online Privacy Protection Act im Bereich der Telekommunikation und der neuen Medien.

Demnach fehlt in den USA ein allgemeines und bereichsübergreifendes Gesetz zum Schutz personenbezogener Daten sowohl für den öffentlichen als auch den privaten Sektor. Auch wenn es im öffentlichen Sektor ein gesamtstaatliches Gesetz gibt, ist dieser Schutz nur begrenzt.

B. Datenschutz bei den konkreten Maßnahmen

Der vierte Verfassungszusatz schützt eine Person gegen unbegründete Durchsuchung und Beschlagnahme, wenn eine Person begründete Erwartung auf *privacy* hat. Ein *warrant*, der auf einen wahrscheinlichen Grund (*probable cause*) gestützt wird, kann eine Durchsuchung durch den Staat rechtfertigen. In den USA wird das Recht auf die informationelle Privatheit zwar verfassungsrechtlich mit Hilfe der Unterscheidung zwischen Vertraulichkeits- und Selbstbestimmungsinteressen überprüft und geschützt, aber die konkreten Vorkehrungen zum Zweck des Schutzes dieses Rechts werden aus den verfassungsrechtlichen Entscheidungen nicht abgeleitet.

410 5 U. S. C. § 552a (b).

Die konkreten Kriterien bzw. Schutzmaßnahmen im Hinblick auf das Recht auf informationelle Privatheit werden eher durch die FIPs[411] oder andere bundesrechtliche Einfachgesetze empfohlen oder ergriffen. Da die *privacy* zwar im Rahmen des vierten Verfassungszusatzes geschützt ist, aber darunter verschiedene Ausnahmen und *privacy doctrines* gelten, ist es sinnvoll zu betrachten, wie die Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten durch den Staat im Rahmen bestimmter Einfachgesetze geregelt werden.

In diesem Zusammenhang soll zuerst untersucht werden, wie das Strafregister, die Rasterfahndung und die Vorratsdatenspeicherung als die für die vorliegende Arbeit ausgewählten Bereiche gesetzlich bestimmt sind und welche Daten darunter auf welche Weise erhoben, gespeichert, verwendet und weitergegeben werden dürfen. Anschließend soll eingeschätzt werden, welche Maßnahmen zum Zweck des Schutzes personenbezogener Daten gegen den unbefugten oder übermäßigen Zugriff darauf getroffen werden und ob die Vorkehrungen hinreichend sind, um den Einzelnen unter den modernen automatisierten Datenverarbeitungsbedingungen zu schützen.

I. Strafregister

Die *criminal history records*[412] spielen eine bedeutsame und oft entscheidende Rolle in jeder Phase des Strafverfahrens.[413] Die USA haben kein national zentralisiertes Strafregister. Vielmehr betreibt jeder Staat ein eigenes zentrales Strafregister, das die Fallverarbeitungsinformationen erhält, zu denen die Strafverfolgungsbehörden, die Gerichte und die Vollstre-

411 Fair Information Practices, in: *U. S. Department of Health, Education & Welfare*, Records, Computers, and the Rights of Citizens: Report of the Secretary's Advisory Committee on Automated Personal Data Systems, 1973.

412 Der United States Code definiert die *criminal history records* als „information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release" (42 U. S. C. § 14616).

413 Die Daten fördern die Entscheidungsfindung in jeder Phase des Strafverfahrens: "to keep track of arrestees; to identify and apprehend absconders; to assess risk of flight and future criminality for purposes of pretrial and post-trial detention; to make prosecutorial decisions on diversion, charging, and plea bargaining; to determine appropriate sentences; and to administer probation, jails, prisons, and parole."

ckungsbehörden des jeweiligen Staats beigetragen haben. Das Strafregister wird den Strafverfolgungsbehörden um legitimer Zwecke willen durch landesweite Telekommunikationssysteme zugänglich gemacht. Infolge des tendenziell zunehmenden Zugangs zu den im Strafregister gespeicherten Daten und der wachsenden Anzahl privater Informationsvermittler mit eigenen Strafregisterdatenbanken wird die Frage des Datenschutzes im Bereich des Strafregisters öfter als je zuvor gestellt.

Bis 1967 betrieb das FBI eine zentralisierte Strafregisterdatei, die als primäre Quelle für den zwischenstaatlichen Datenaustausch bei nationalen Strafregisteranfragen diente. Das FBI behielt in seiner eigenen Datenbank Kopien der *rap sheets*[414] aller Staaten, damit eine Strafverfolgungsbehörde in einem Staat herausfinden konnte, ob eine bestimmte Person in einem Strafregister eines anderen Staates registriert war. Als eine Reaktion auf den Vorschlag der *President's Commission on Law Enforcement and Administration of Justice*[415] gründete das FBI 1967 das *National Crime Information Center* (NCIC) unter der *Criminal Justice Information Services Division* (CJISD), um eine bundesweite, benutzerorientierte Computerauskunft aus dem Strafregister zur Verfügung zu stellen. Daraufhin führte das NCIC ein zwischenstaatliches computergestütztes Strafregistersystem – *an interstate computerized criminal history record system* (CCH-System) – ein, das Angaben über Personen enthält, die wegen Verbrechen und schwerer Vergehen unter dem Gesetz des Bundes- bzw. Einzelstaats verhaftet wurden. Der National Crime Prevention and Privacy Compact Act von 1998 sah vor, dass das Informationssystem des FBI verschlankt und damit in einen effizienteren *Interstate Identification Index* (Triple I-System oder III-System) umgewandelt wird. Die Besorgnis über die Idee, ein nationales zentralisiertes Strafregister zu etablieren, sowie die Besorgnis um seine Praktikabilität und die Kosten führten nämlich dazu, dass das FBI das CCH-Programm zugunsten des dezentralisierten nationalen III-Systems[416] beendete.

---

414 Das bedeutet eine Chronologie der Handlungen des Strafjustizsystems in Bezug auf eine bestimmte Person, einschließlich Verhaftungen, Anklagedaten, Urteilen und Verurteilungen (*Jacobs*, Mass Incarceration and the Proliferation of Criminal Records, Vol. 3 Issue 3, Univ. Of St. Thomas Law Journal, S. 392).

415 President's Commission on Law Enforcement and Administration of Justice, The Challenge of Crime in a Free Society (Washington D. C.: Government Printing Office, February 1967).

416 Das *Interstate Identification Index System* oder das III-System ist das kooperative *federal state system* für den Austausch von Angaben aus dem Strafregister und umfasst den *National Identification Index*, die Nationale Fingerabdruck-Datei und die *criminal history record repositories* der Einzelstaaten in dem Ausmaß ihrer

1. Organisationsstruktur

Das III-System ist ein zwischenstaatliches Computernetzwerk, das unter anderem dem Datenaustausch zwischen dem Bund und den Einzelstaaten dient und das die Mittel zur Verfügung stellt, mit denen beim nationalen Strafregister angefragt wird, um festzustellen, ob eine Person in einem der Bundesstaaten registriert ist.[417] Das NCIC pflegte bis vor Kurzem in der eigenen Datenbank Kopien von *rap sheets* aller Einzelstaaten, sodass eine Strafverfolgungsbehörde in einem Staat herausfinden konnte, ob ein Verhafteter oder eine Person von Interesse (wie ein Verdächtiger) in einem anderen Staat eine Eintragung in einem staatlichen Strafregister hatte.[418] Die Sorge um die Kosten sowie die Effizienz aufgrund des doppelten nationalen Registers von einzelstaatlichen Täterdatensätzen,[419] die Notwendigkeit zur Schaffung eines dezentralisierten nationalen Strafregistersystems mit gemeinsamer Verantwortung und gegenseitiger Verpflichtung[420] und der erhebliche technische und organisatorische Fortschritt, der ein dezentralisiertes nationales Strafregister unterstützen kann, führten dazu, dass das III-System das zentralisierte Datenbanksystem ersetzte.

Das III-System ist dazu gedacht, die automatisierten Datenbanken der staatlichen zentralen Strafregister und des FBI durch einen *Index-Pointer-Ansatz* in ein nationales System zusammenzuführen. Das FBI führt nun in erster Linie ein 51. Strafregister und stellt dabei Informationen über Bundesstraftäter zur Verfügung. Staatliche Strafregister, die als Datenanbieter für nationale III-Suchzwecke funktionieren, übernehmen die Verantwortung für die Bereitstellung von *criminal history records* online in Re-

---

Teilnahme an diesem System und das *criminal history record repository* des FBI (28 C. F. R. § 20.3 (m)).

417 Über das dezentrale III-System siehe unten Schaubild 1.

418 Zur frühen Entwicklung dieses Programms siehe U. S. Dept. of Justice v. Reporter's Committee for Freedom of Press.

419 Dies ist vor allem darauf zurückzuführen, dass die Einreichung von Verhaftungs- und Verfügungsinformationen an die staatlichen *repositories* durch staatliche und örtliche Justizbehörden in den meisten Staaten gesetzlich vorgeschrieben ist, während die Einreichung dieser Informationen beim FBI durch diese Behörden freiwillig ist.

420 28 C. F. R. § 20.37: "It shall be the responsibility of each criminal justice agency contributing data to the III System and the FIRS to assure that information on individuals is kept complete, accurate, and current so that all such records shall contain to the maximum extent feasible dispositions for all arrest data included therein. Dispositions should be submitted by criminal justice agencies within 120 days after the disposition has occurred."

aktion auf III-Datenanfragen für Strafverfolgungszwecke. Dafür erlauben alle staatlichen Gesetzgebungen bezüglich *criminal history records* den zwischenstaatlichen und den zwischen dem Bund und den einzelnen Staaten stattfindenden Datenaustausch.

Das Verfahren der Mitteilung und Speicherung von Datensätzen im dezentralen III-System ist je nach den am NFF teilnehmenden oder nicht teilnehmenden Staaten unterschiedlich.[421] Im Fall von NFF-Staaten leitet deren Strafregister dem FBI bei der Verhaftung einer Person, die noch nie zuvor im Staat verhaftet wurde, die Fingerabdrücke der Person zusammen mit den Textdokumenteninformationen weiter. Die Identifikationsinformationen werden verwendet, damit die Person zum NII hinzugefügt oder der Index aktualisiert werden kann. Wenn die Person bereits im Index ist, dienen die Daten zur Festlegung eines Pointer, der angibt, dass das Repository einen *criminal history record* über die für berechtigte III-Zwecke zur Verfügung stehende Person enthält. Die Fingerabdrücke werden dem NFF hinzugefügt. Die Einzelstaaten senden also nur die erste Verhaftungseintragung elektronisch an das FBI, die im *Interstate Identification Index* der Aktualisierung der Liste von Tätern und Staaten dient, die weitere konkrete Registrierungen haben.[422] Weitere strafrechtlich relevante Daten, die sich auf die Täter beziehen, speichern die Staaten selbst. Damit stellen sie die Strafregistrierungen und die damit zusammenhängenden Informationen für eventuelle Anfragen aus anderen Einzelstaaten oder von zugelassenen Bundesbehörden zur Verfügung. Wenn eine Person verhaftet wird, die bereits zuvor in dem jeweiligen Staat verhaftet wurde, und wenn für die Übermittlung der staatlichen Verurteilungsdaten zum III-Zwecke das staatliche Repository zuständig ist, werden die Fingerabdrücke oder

421 NFF (*National Fingerprint File*) ist eine Datenbank von Fingerabdrücken oder anderen eindeutigen persönlichen Identifizierungsinformationen, die sich auf eine verhaftete oder angezeigte Person beziehen. Die darin enthaltenen Daten werden vom FBI gepflegt, um eine positive Identifizierung von Daten, die im III-System indiziert sind, zu pflegen (28 C. F. R. § 20.3 (o)). Die Staaten, die die Verantwortung für die Bereitstellung ihrer III-indizierten *criminal history records* sowohl für nicht strafjustizielle Zwecke als auch für Strafjustizzwecke übernommen haben, werden als „NFF-Staaten" bezeichnet, weil sie dem FBI dem *National Fingerprint File-Konzept* gemäß Fingerabdrücke und Anzeigen- sowie Dispositionsinformationen von Straftätern vorlegen. Bis zum Jahresende 2016 haben 20 Staaten am NFF teilgenommen (http://www.search.org/states-participation-in-national-systems-and-programs-that-facilitate-interstate-exchange-of-criminal-history-records/, abgerufen am 29. Juni 2018).

422 Zurzeit nehmen alle fünfzig Staaten und der District of Columbia am III-System teil.

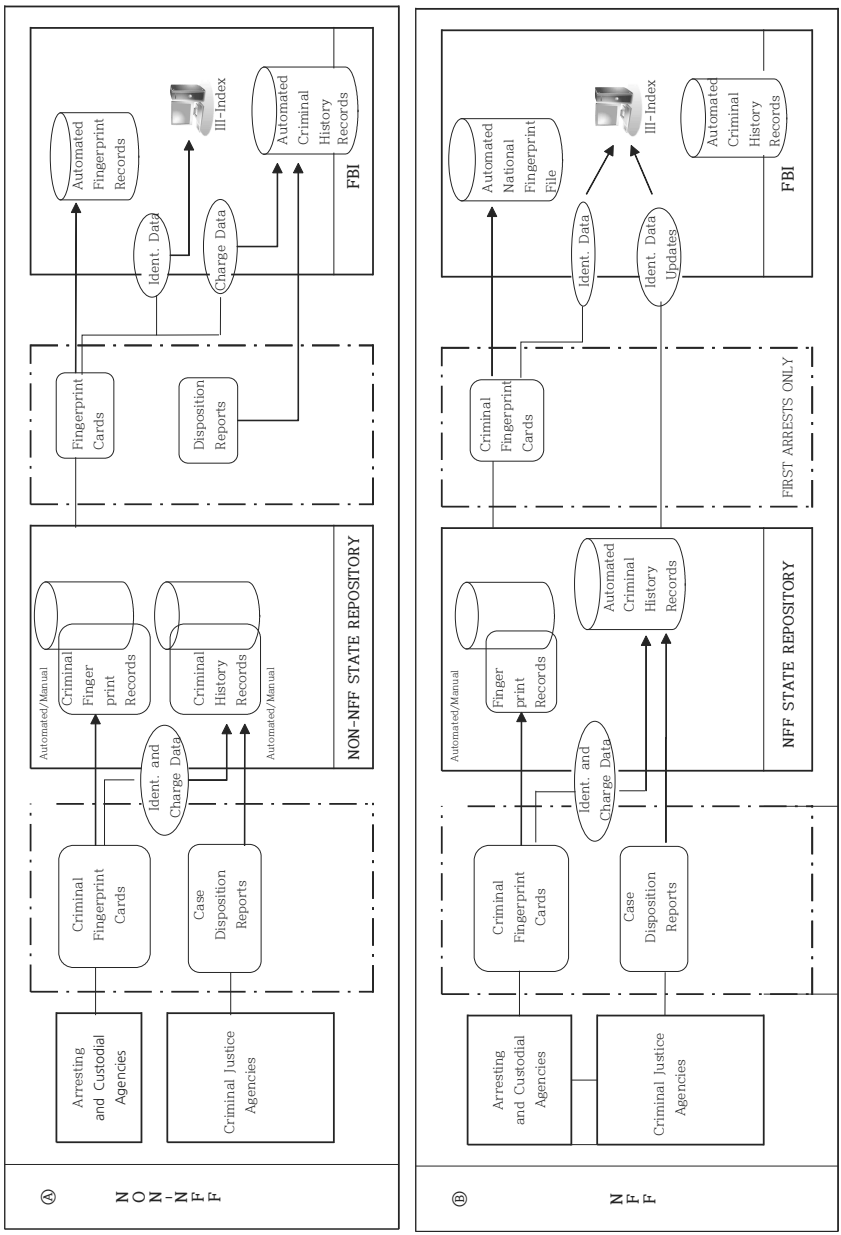
Anzeigen-/Dispositionsdaten nicht an das FBI weitergeleitet. Wenn eine Person verhaftet wird, die zwar bereits zuvor in dem jeweiligen Staat verhaftet wurde, aber für die Übermittlung ihrer staatlichen Eintragungen im Repository zum III-Zwecke das FBI verantwortlich ist,[423] leitet das einzelstaatliche Register die Fingerabdrücke oder Anzeigen-/Dispositionsdaten nach Vor-NFF-Praktiken weiter, sodass das FBI seine Eintragungen aktuell halten kann. Die Nicht-NFF-Staaten leiten ähnlich wie beim dritten Verfahren alle Fingerabdrücke oder Anzeigen-/Dispositionsdaten an das FBI weiter.

Unter diesem Ansatz unterhält das FBI einen automatisierten Master-Name-Index (MNI),[424] den *National Identification Index* (NII), der Namen und Identifikationsdaten enthält, die alle Personen betreffen, deren automatisierte Registrierungen über das III-System verfügbar sind.

423 Während sich einige III-Staaten darauf verständigt haben, nur die Aufzeichnungen von Personen zur Verfügung zu stellen, die als Ersttäter im Staat nach dem Zeitpunkt verhaftet und/oder angezeigt wurden, ab dem die Teilnahme am III-System stattfand, übernahmen die anderen Strafregister die Verantwortung für neue erstmalige Strafregistrierungen sowie für einige bereits vorhandene Aufzeichnungen von In-State-Straftätern. Das FBI stellt weiterhin einige Aufzeichnungen von Personen in III-Staaten zur Verfügung, deren Aufzeichnungen nicht auf staatlicher Ebene automatisiert wurden (vor allem ältere Personen, die vor Kurzem nicht kriminell tätig waren).

424 The master name index (MNI) is a key element of the criminal history system of the National Instant Criminal Background Check System (known as *NICS*) used for point-of-sale background checks of potential gun purchasers because it permits the user to identify a felony flag on a record of a named offender.

Schaubild 1: Berichterstattung und Pflege von Strafregistrierungen in einem dezentralen III-System[425]



2. Inhalt des Registers

Nach dem US-Code umfasst der Begriff der *criminal history records* nicht nur die strafgerichtlichen Verurteilungsdaten, sondern auch die Daten von Verhaftungen, die nicht zu einer Verurteilung führten, etwa in Fällen, in denen das Hauptverfahren nicht eröffnet wurde[426] oder in denen der Angeklagte vor Gericht freigesprochen wurde.[427] Alle Staaten speichern danach neben den strafgerichtlichen Verurteilungsdaten auch die Verhaftungsdaten in ihren Strafregistern, obwohl sich die in ihr Strafregister einzutragenden Inhalte gesetzlich unterschiedlich gestalten.

In den USA sieht kein Bundesgesetz vor, was in die staatlichen Strafregister eingetragen werden soll. Unabhängig von den einzelnen staatlichen Regelungen über die Inhalte des Registers werden auf bundesgesetzlicher Ebene nur die unter dem III-System zur Verfügung stehenden Zielverbrechen und die konkreten Angaben vorgesehen. Die *criminal history record information*, die im III-System und im *Fingerprint Identification Records System* (FIRS) gepflegt wird, umfasst in der Regel nur schwere und/oder erhebliche Straftaten von Erwachsenen und Jugendlichen. Das heißt, das FBI akzeptiert nach dem geltenden Recht keine Fingerabdrücke und Verhaftungsdaten für weniger schwere Straftaten wie z. B. Trunkenheit, Vagabundentum, Friedensstörungen, Bummeln, falsche Feueralarme und

425 Siehe *U. S. Department of Justice*, Use and Management of Criminal History Record Information: A Comprehensive Report, 2001 Update, Bureau of Justice Statistics, S. 86.

426 Während in Deutschland nach dem Legalitätsprinzip die Strafverfolgungsbehörde dazu verpflichtet ist, ein Ermittlungsverfahren zu eröffnen, sobald sie Kenntnis von einer (möglichen) Straftat erlangt hat, können die Strafverfolgungsbehörden in den USA auf ein Opportunitätsprinzip zurückgreifen. Die Hauptaufgabe des Staatsanwalts im Vorverfahren besteht darin, die Flut der von der Polizei weitergeleiteten Fälle in einer nach der Verurteilungswahrscheinlichkeit und Verfolgungswürdigkeit gerichteten Prüfung zügig und wenn möglich ohne Durchführung einer nach dem amerikanischen Recht sehr aufwendigen Hauptverhandlung zu erledigen. Dabei kann sich der Staatsanwalt zur Bewältigung dieser Aufgabe ebenfalls auf einen weiten, kaum überprüfbaren Ermessensspielraum berufen. Er kann Anklage erheben oder eine der vielen ihm zur Verfügung stehenden Arten der vorzeitigen, bedingten oder endgültigen Verfahrenseinstellung wählen (siehe *Lützner*, USA, in: *Gropp* (Hrsg.), Besondere Ermittlungsmaßnahmen zur Bekämpfung der Organisierten Kriminalität, S. 743).

427 Siehe auch oben Fn. 412.

Verkehrsverstöße.[428] Auf der einzelstaatlichen Ebene werden die Fingerabdrücke oder *criminal records* von Personen, die wegen solcher Straftaten verhaftet wurden, in einigen Staaten[429] gesammelt, aber in anderen nicht.[430] Auch wenn ein staatliches Register die *criminal records* der wegen minder schwerer Straftaten verhafteten Personen enthalten haben könnte, können die nicht in demselben Staat ansässigen Justizbehörden die Daten nicht durch eine Suche in der NCIC herausfinden.[431] Die einzelstaatlichen sowie das bundesstaatliche Strafregister speichern in der Regel die folgenden Informationen: Identifizierungsinformationen von Personen, auf die sich Angaben beziehen, sowie Informationen bezogen auf aktuelle und frühere Strafjustizverfahren (einschließlich Verhaftungen oder anderer formaler Strafanzeigen und Verfügungen, die von diesen Verhaftungen oder formellen Anklagen geführt werden). Erstere umfassen in der Regel die folgenden Angaben: Name, Adresse, Geburtsdatum, Sozialversicherungsnummer, Geschlecht, ethnische Zugehörigkeit, physikalische Eigenschaften wie Haar- und Augenfarbe, Größe, Gewicht und auffällige Narben oder Tattoos, insbesondere auch die Fingerabdrücke.[432] Letztere enthalten Informationen über alle Verhaftungen mit den verfügbaren Dispositionsdaten.

Das FBI führt kein gesondertes Strafregister für Jugendliche, es sei denn, dass sie als Erwachsene vor Gericht stehen. Bis 1992 wurden Gerichtsentscheidungen über Jugendliche nicht in der NCIC-Datenbank des FBI gespeichert. Ein dramatischer Anstieg der Jugendkriminalität führte allerdings dazu, dass der Generalstaatsanwalt eine Regel implementiert hat, die das FBI dazu ermächtigt, die *criminal records* für schwere Straftaten von

428 28 C. F. R. § 20.32 (a) und (b). Das FBI schlug jedoch vor, in das NCIC alle Verhaftungen einschließlich der weniger schweren Straftaten und der Vergehen im jugendlichen Alter einzubeziehen. Es vertrat die Erweiterung des Strafregisterumfangs aus zwei Gründen: erstens, um eine einheitliche nationale Politik zu schaffen, sodass Strafverfolgungsbehörden und Arbeitgeber, die ein FBI-criminal-history-record suchen, in einem anderen Staat die gleichen Informationen erhalten wie Strafverfolgungsbehörden und Arbeitgeber in dem Staat, in dem das Strafregister registriert wurde; und zweitens, um den öffentlichen und privaten Arbeitgebern wertvolle Informationen über potenzielle Mitarbeiter zu geben (*Jacobs/Crepet*, The Expanding Scope, Use and Availability of Criminal Records, Legislation and Public Policy, Vol 11, 2008, 177, 188 und m. w. N.).

429 Siehe z. B. Ohio Rev. Code Ann. § 109.60.

430 Siehe z. B. N. Y. Crim. Proc. Law § 160.10.

431 28 C. F. R. § 20.32 (b).

432 Daneben dürfen auch Arbeitsplatzadresse, Automobilregistrierung und andere relevante Informationen gespeichert werden.

Jugendlichen in einzelstaatliche Strafregister einzutragen. Im Dezember 1992 kündigte das FBI an, dass die Jugendkriminalitätsangaben gemäß der neuen Regel unter den gleichen Standards übermittelt werden, die für die Verbreitung von normalen Strafregisterangaben (Erwachsene) gelten.

Ein Problem bezüglich der Datenspeicherung in einzelstaatlichen Strafregistern lösen die schlichten Strafverfahrensdaten – *arrest records* – aus, die nicht zur Verurteilung geführt haben. Die Daten werden zwar unter dem III-System zwischen einem die Daten erhaltenden Staat und einem anderen Staat nicht ausgetauscht. Die Speicherung der Strafverfahrensdaten ohne Verurteilung erfolgt jedoch auch dann, wenn ein Hauptverfahren gegen einen bestimmten Beschuldigten nicht eröffnet oder er für unschuldig erklärt wird, was für den ehemals zu Unrecht Beschuldigten zu nachteiligen Folgen führt.[433]

3. Verwendung der Daten aus dem Register

Im Grunde genommen sind die Bundesbehörden gesetzlich und verfassungsrechtlich dazu verpflichtet, sowohl die Daten der Öffentlichkeit zugänglich zu machen als auch die *privacy* personenbezogener Daten über die Personen in den Datenbanken zu schützen.[434] Die Entscheidung über den Schutz der *privacy* von Gerichtsdaten liegt im Allgemeinen im Ermessen der Richter und es besteht die Vermutung des öffentlichen Zugangs zu diesen Gerichtsdaten. Es liegt auch im Ermessen der Gerichte, bestimmte Gerichtsverfahren oder Teile von Gerichtsverfahren vor der Öffentlichkeit zu schützen. Die *privacy* anderer staatlicher Daten wird in erster Linie durch den Freedom of Information Act (FOIA), das zur Förderung der Transparenz in nationalen Datenspeicherungssystemen dient, und durch die einzelstaatlichen vergleichbaren Gesetze geregelt. Nach diesen Gesetzen kann jede Person Daten von Bundesbehörden anfordern.[435] Parallel

433 Siehe unten 4. über die möglichen Nachteile der Strafverfahrensdatenspeicherung.

434 *Solove/Schwartz*, Privacy Law: Fundamentals, S. 55 f.

435 Viele dieser Gesetze sehen Ausnahmen für die Offenlegung vor, um die *privacy* zu schützen. Das FOIA enthält neun Ausnahmen zur Offenlegung: (1) als vertraulich eingestufte Daten; (2) interne Personalregeln und -praktiken; (3) gesetzlich ausgenommene Daten; (4) Geschäftsgeheimnisse und vertrauliche Daten; (5) bestimmte Verhandlungsmaterialien; (6) Personal- und Krankenakten sowie ähnliche Akten, deren Offenlegung eine ungerechtfertigte Verletzung der *privacy* darstellen würde; (7) Strafverfolgungsdaten, die Rechtsstreitigkeiten stören,

dazu regelt der Privacy Act die Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten durch die Bundesbehörden. Das Gesetz erstreckt sich aber nicht auf den privaten Sektor oder einzelstaatliche Behörden.

Die Gerichte haben jedoch entschieden, dass verfassungsrechtliche Privacy-Grundsätze nur geringe Auswirkungen auf die Erhebung, Speicherung oder Übermittlung von *criminal history record information* durch Strafverfolgungsbehörden haben.[436] Die Verfassung erkennt zwar ein berechtigtes Interesse an der *privacy* sensibler persönlicher Daten an,[437] der U. S. Supreme Court hat später jedoch festgestellt, dass die verfassungsrechtlichen Privacy-Grundsätze die Übermittlung von Daten über offizielle Handlungen durch Strafverfolgungsbehörden wie etwa eine Verhaftung nicht einschränken.[438] *Common Law Privacy Doctrines* haben sich daraufhin als weitgehend irrelevant für die Verwaltung von *criminal history record information* erwiesen.[439] Das führt zu einem Flickenteppich einer Vielzahl von Bundes- und Landesgesetzen und -rechtsverordnungen, die die Erhebung, Speicherung, Verwendung und Weitergabe von Strafregistrierungen regeln. Auf Bundesebene haben das Parlament mit einem Gesetz[440] und das Justizministerium mit einer Verordnung[441] Mindestanforderungen für die Verwaltung von *criminal history record systems* festgelegt, wobei es den Einzelstaaten überlassen wird, spezifischere Gesetze und Vorschriften zu entwickeln, um sicherzustellen, dass die staatlichen *criminal history records* vollständig, genau, für berechtigte Nutzer leicht zugänglich und vertrauenswürdig sind. Zur Sicherstellung der Vollständigkeit, der Genauigkeit und der Sicherheit von Strafregistrierungen, die die Strafregister erheben,

---

in die *privacy* eindringen, vertrauliche Quellen preisgeben oder die Sicherheit von Personen gefährden würden; (8) bestimmte Daten im Zusammenhang mit der Beaufsichtigung von Finanzinstituten; (9) geologische und geophysikalische Daten in Bezug auf *wells*.

436 Siehe *U. S. Department of Justice*, Use and Management of Criminal History Record Information: A Comprehensive Report, 2001 Update, Bureau of Justice Statistics, S. 45.

437 Whalen v. Roe, 429 U. S. 589.

438 Paul v. Davis, 424 U. S. 693 (713).

439 *U. S. Department of Justice*, Use and Management of Criminal History Record Information: A Comprehensive Report, 2001 Update, Bureau of Justice Statistics, S. 45.

440 Omnibus Crime Control and Safe Streets Act of 1968, 42 U. S. C. § 3789g (b), as amended by § 524 (b) of the Crime Control Act of 1973, Pub. L. No. 93-83, 87 Stat. 197 (1973).

441 28 C. F. R. § 20.21 (a) (1).

speichern und übermitteln, wurden mehrere gesetzliche Maßnahmen getroffen. Um die Vollständigkeit, die Genauigkeit und die Sicherheit der Daten sicherzustellen, werden per Gesetz und Verordnung einige Maßnahmen auf Bundesebene gefordert. Die gesetzliche Befugnis des Federal Bureau of Investigation (FBI) zur Verwaltung von Strafregistrierungen findet sich vor allem in 28 U. S. C. § 534. Insbesondere wird der Generalstaatsanwalt gemäß den Absätzen (a) (1) und (a) (4) dazu ermächtigt, Personalien sowie die kriminalistisch relevanten und andere Daten zu erheben, zu speichern, zu klassifizieren und aufzubewahren sowie solche Daten mit den befugten Behörden zu teilen.[442]

Die Daten, die von einem *Central State Repository* gepflegt werden, sind zu ihrer Vollständigkeit innerhalb von 90 Tagen nach den Verfügungen zu erheben und zu speichern. Auf einzelstaatlicher Ebene ist die obligatorische Mitteilung von Verhaftungs- und Verfügungsdaten in allen Einzelstaaten geregelt, damit die Datenqualität sichergestellt werden kann. Zur Genauigkeit sollen Strafverfolgungsbehörden einen Prozess der systematischen Prüfung im Rahmen der Datenerhebung, der Eintragung und der Speicherung einleiten, der die Möglichkeit der Aufzeichnung und Speicherung ungenauer Informationen minimiert, und sie sollen alle Strafverfolgungsbehörden, die bereits solche Informationen erhalten haben, auch nachträglich benachrichtigen, wenn sie unzutreffende Informationen finden.[443] Teile der Verordnung wurden in den nationalen Gesetzen aller Länder umgesetzt, doch das gilt nicht für alle Teile. Manche wurden nur in den nationalen Gesetzen einiger, aber nicht aller Länder umgesetzt.[444]

Unter dem dezentralen Strafregisterwesen mit dem III-System unterscheiden sich die Regelungen über den Zugang zu und der Auskunftserteilung von Daten aus dem Strafregister von Staat zu Staat. Das Verfahren

---

442 Weitere bundesstaatliche Gesetze und Verordnungen, die den Generalstaatsanwalt zur Übermittlung von Strafregistern ermächtigen, sind PL 99 -169, as amended by PL 99 – 569 and PL 101 – 246, 5 U. S. C. § 9101; Executive Orders 10450 and 12968; PL 91 – 452; PL 101 – 647; PL 92 – 544, 86 Stat. 1115; PL 100 – 413; 102 Stat. 1101; PL 94 – 29, as amended by PL 100 – 181, 15 U. S. C. § 78q (f)(2); PL 97 – 444, 7 U. S. C. §§ 12a, 21 (b)(4)(e); PL 99 – 399, 42 U. S. C. § 2169; PL 101 – 604, 49 U. S. C. 44936; 28 C. F. R. 0.85 (b); U. S. Dep´t of Justice Order 556 – 73, 28 C. F. R. 16.30 – 16.34; 5 C. F. R. 732 & 736; PL 103 – 159; PL 103 – 209; PL 103 – 322.

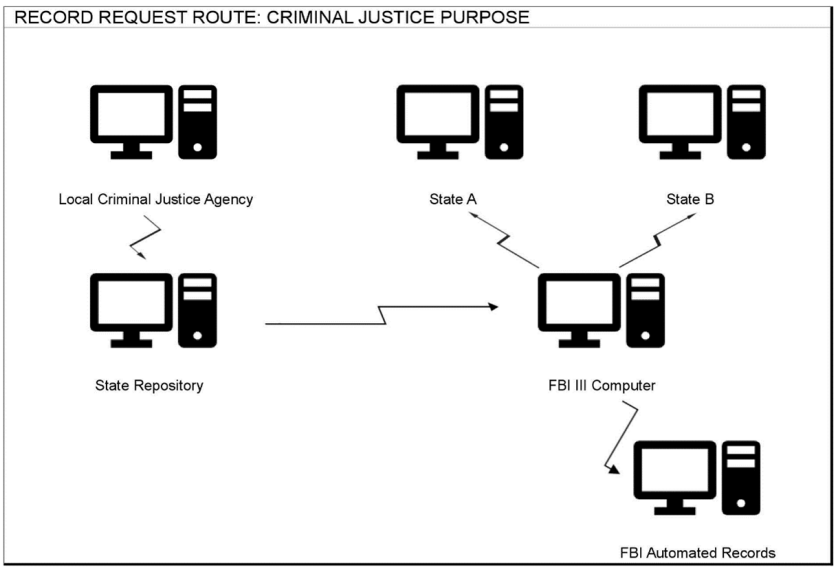
443 28 C. F. R. § 20.21 (a).

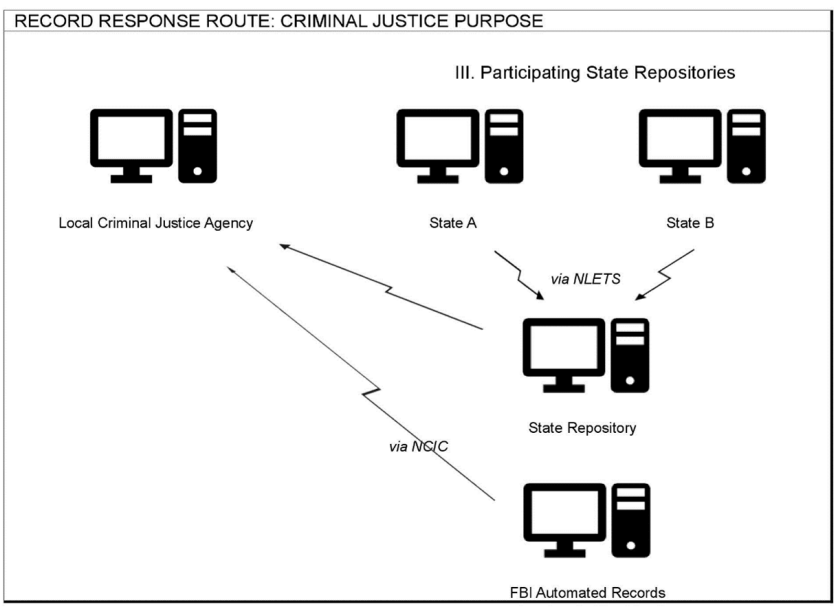
444 *U. S. Department of Justice*, Use and Management of Criminal History Record Information: A Comprehensive Report, 2001 Update, Bureau of Justice Statistics, S. 49 ff.

einer Anfrage und Auskunft läuft grundsätzlich jedoch wie folgt ab:[445] Eine lokale Justizbehörde überträgt die Anfrage über das staatliche Telekommunikationsnetz an das staatliche Register. Das Register leitet die Anfragenachricht über das NCIC-Netzwerk an den III-Computer weiter. Der III-Computer schaltet die Meldungen entweder auf das staatliche Strafregister um, das Strafregistrierungen über die die Anfrage betreffenden Personen beinhaltet, und/oder auf das FBI, wenn es bezüglich der fraglichen Personen einen Datensatz auf Bundesebene oder in einem oder mehreren Staaten gibt, die nicht am III-System teilnehmen. Wenn das Ergebnis einer Suche nach diesem Index zeigt, dass das Suchthema eine III-indizierte Registrierung hat, wird der Index auf die anfragende Behörde an das FBI und/oder an eine oder mehrere der staatlichen Strafregister verweisen, von denen der Datensatz oder die Datensätze dann übermittelt werden. Die anfragende Behörde kann die Registrierungen dabei mit Hilfe des NCIC-Netzwerks und des *National Law Enforcement Telecommunications System* (NLETS Network) direkt aus den angegebenen Quellen erhalten. Genauer gesagt werden Angaben, die von den automatisierten Dateien des FBI geliefert werden, über das NCIC-Netzwerk an das anfragende staatliche Register zurückgegeben. Die am III-System teilnehmenden staatlichen Strafregister nutzen das NLETS-Netzwerk, um Auskünfte zu erteilen. Das die Auskünfte erhaltende staatliche Strafregister gruppiert, falls erforderlich, mehrstaatliche Angabenkomponenten und übermittelt eine Antwort an die anfragende Behörde. Der gesamte Prozess dauert in der Regel weniger als eine Minute.

445 Über das Verfahren einer Datenanfrage und -auskunft für strafjustizielle Zwecke siehe unten Schaubild 2.

Schaubild 2: Datenanfragen und -antworten für strafjustizielle Zwecke[446]





Für die Übermittlung personenbezogener Daten gelten je nach der über sie Auskunft erhaltenden Behörde und den Zwecken unterschiedliche Einschränkungen.[447] Nach 28 C. F. R. § 20.21 (b) und (c) gibt es Beschränkungen nur bei der Übermittlung von *nonconviction data* (Verhaftungsdaten, die nicht zu einer Verurteilung führen) und bei der Übermittlung an die *noncriminal justice agencies*. Die Beschränkung gilt also weder für die Übermittlung von Verurteilungsdaten noch für die Übermittlung von *criminal history records* an Strafjustizbehörden. Dementsprechend stellen die Staaten in der Regel nur wenige oder keine Beschränkungen für die Übermittlungen von Verurteilungsdaten vor, und eine Reihe von Staaten beschränken auch nicht die Übermittlung von *open arrest records*, die weniger als ein Jahr alt sind.[448] Die Mehrheit der strafjustiziellen Anfragen an staatliche Strafregister für *criminal history records* wird von entfernten Computer-Terminals online empfangen. Solche Online-Remote-Terminals bieten einen direkten Zugriff auf das MNI des Repository für die Durchführung von Suchvorgängen und für die Führung von *criminal history files* zum Zweck der Erlangung von c*riminal history records*. Hierbei wird auf der föderalen Ebene die Führung der staatlichen Strafregister nur unter dem Aspekt der Vollständigkeit, der Genauigkeit und der Sicherheit von Daten kontrolliert, die von staatlichen Registern gespeichert und gepflegt werden, nicht aber unter dem Aspekt des Datenschutzes. Generell gibt es so gut wie keine datenschutzrechtlichen Regelungen in diesem Bereich.

Neben der Nutzung der Daten aus dem Strafregister zu strafrechtlichen Zwecken wurde der Zugriff auf die Datensätze aus dem Strafregister erweitert. Die *criminal records* werden nicht nur den lokalen, staatlichen und föderalen Strafverfolgungsbehörden zur Verfügung gestellt, sondern

446 Siehe *U. S. Department of Justice*, Use and Management of Criminal History Record Information: A Comprehensive Report, 2001 Update, Bureau of Justice Statistics, S. 78.

447 28 C. F. R. § 20.33 (a).

448 *U. S. Department of Justice*, Use and Management of Criminal History Record Information: A Comprehensive Report, 2001 Update, Bureau of Justice Statistics, S. 55.

sind auch anderweitig verfügbar.[449,450] Eine zunehmende Anzahl von Staaten erleichtert es jeder Person, für irgendeinen Zweck die Daten über irgendjemanden aus dem Strafregister zu erhalten.[451] Der hauptsächliche Grund dafür ist die Gesetzgebung, die die durch den Bund veranlassten *background checks* (Hintergrundprüfungen) für nichtstrafrechtliche Zwecke ermöglicht oder erfordert, und Megans Gesetze. Insbesondere für Sexualstraftäter stehen aufgrund der Verbreitung von Megans Gesetzen und des *Adam Walsh*-Gesetzes personenbezogene Daten aus dem Strafregister kostenlos online zur Verfügung.[452] Darüber hinaus wurde die Vertraulichkeit einzelner Strafregisterdaten durch die Verabschiedung von Gesetzen zu Hintergrundprüfungen erheblich beeinträchtigt.

Megans Gesetze, die die Identitäten, Adressen und Straftaten von Sexualstraftätern über das Internet öffentlich zugänglich machen, haben ebenfalls zu einem rascheren Zugang zu staatlichen Strafregistern geführt.[453]

---

449 Die staatlichen Strafregister machen ihre *criminal records* nicht nur der staatlichen und lokalen Polizei, Bewährungsbehörde, Strafvollzugsbehörde und den anderen Strafjustizbehörden, sondern auch einigen Arbeitgebern und Verbänden verfügbar: S. Colo. Rev. Stat. § 24-72-303 (2007); *U. S. Department of Justice*, Survey of State Criminal History Information Systems, 2003, Bureau of Justice Statistics.

450 Die Verurteilungsdaten stehen gegen eine Gebühr zur Verfügung oder sind sogar frei online zugänglich. So veröffentlicht z. B. Colorado alle Verurteilungen im Internet und ermöglicht gegen eine geringe Gebühr die Durchführung einer Strafregistersuche über das Internet. Connecticut macht Verurteilungsdaten für die Öffentlichkeit allgemein zugänglich. Kansas, Montana und Oklahoma verlangen bereits von bestimmten gewalttätigen Tätern, sich bei der Strafvollzugsbehörde oder einer lokalen Strafverfolgungsbehörde anzumelden. Ein in Illinois verabschiedetes Gesetz weist staatliche Feuerwehrstationen an, auf ihrer Webseite Daten über Brandstifter zu veröffentlichen. Tennessee stellt jeder Person gegen eine Gebühr eine Kopie aller Verurteilungsdaten in seinem Strafregister zur Verfügung. Viele Staaten, einschließlich Florida, bieten den Online-Zugang zu einem Namensverzeichnis von aktuellen und ehemaligen staatlichen Gefangenen (vgl. *Jacobs*, Mass Incarceration and the Proliferation of Criminal Records, Vol. 3 Issue 3, Univ. Of St. Thomas Law Journal, S. 399 f.).

451 *U. S. Department of Justice*, Report of the National Task Force on Privacy, Technology, and Criminal Justice Information, 2001, Bureau of Justice Statistics, S. 1.

452 Ein obligatorisches Anmelde- und Gemeinschaftsmeldungsgesetz, das von Personen, die wegen Sexual- und Kindermissbrauchsdelikten verurteilt oder wegen seelischer Störung freigestellt wurden, verlangte, sich bei den örtlichen Strafverfolgungsbehörden anzumelden (N. J. Stat. Ann. §§ 2C:7-1-17 (2006).

453 *Jacobs*, Mass Incarceration and the Proliferation of Criminal Records, Vol. 3 Issue 3, Univ. Of St. Thomas Law Journal, S. 399.

Im Jahr 1990 verabschiedete der US-Bundesstaat Washington den ersten Community Protection Act, mit dem die Registerbehörden dazu ermächtigt wurden, Auskünfte über Sexualstraftäter an die Öffentlichkeit zu geben.[454,455] Darüber hinaus garantiert der Adam Walsh Child Protection and Safety Act,[456] dass jeder Staat ein Online-Sexualstraftäterregister haben wird. Das Gesetz sieht vor, dass der US-amerikanische Generalstaatsanwalt die Richtlinien für staatliche Sexualstraftäterregister verkündet, und es droht Staaten an, die die Anforderungen der Registrierungspflicht bis 2009 nicht erfüllen, mit dem Verlust von Bundesförderungen.[457] Das Gesetz fordert ferner, dass das FBI ein nationales Register für Sexualstraftäter einrichtet und führt, das alle staatlichen Register vereint.[458]

Die Vertraulichkeit der *criminal history records* wurde mit der Verabschiedung von Gesetzen, die die föderal-initiierten *background checks* für nicht strafrechtliche Zwecke ermöglichten oder erforderten, ernsthaft erodiert.[459] Die Anzahl der Übermittlung von Fingerabdrücken an das FBI zum Zweck der nicht strafrechtlichen Kontrolle übersteigt nun die Anzahl derer zum Zweck der strafrechtlichen Kontrolle. Im Jahre 2005 wurden etwa zehn Millionen nicht strafrechtliche Kontrollen durchgeführt.[460] Das FBI behandelte die *criminal history records* historisch als so vertraulich, dass sie nur mit lokalen einzelstaatlichen und bundesstaatlichen Strafverfolgungsbehörden geteilt werden sollten.[461] In den letzten Jahren hat das

454 Wash. Rev. Code Ann. § 4.24.550 (West 2005).

455 Nachdem New Jersey als Reaktion auf die Vergewaltigung und Ermordung der siebenjährigen Megan Kanka durch einen zuvor zweimal verurteilten Sexualstraftäter ein Gesetz zur Registrierung von Sexualstraftätern und zur Benachrichtigung der Gemeinschaft verabschiedet hatte, galten Megans Gesetze im ganzen Land. Heute haben alle fünfzig Staaten Megans Gesetze, die es jedem ermöglichen, auf einer Webseite der staatlichen Strafregister für Sexualstraftäter nach einem Namen oder einem Wohnsitz zu suchen (Siehe *Jacobs/Crepet*, The Expanding Scope, Use and Availability of Criminal Records, Legislation and Public Policy, Vol 11, 2008, 177, 205 m. w. N.).

456 Pub. L. No. 109-248, 120 Stat. 587 (2006) (codified as amended in scattered sections of 18 and 24 U. S. C.).

457 Adam Walsh Child Protection and Safety Act §§ 112, 125, 120.

458 Adam Walsh Child Protection and Safety Act § 119.

459 Das Gesetz, das das Parlament im Jahre 1972 erlassen hat, ermöglicht den Bundesstaaten darüber hinaus, dass ihre Strafregister im Namen privater Arbeitgeber die FBI-Hintergrundkontrolle (FBI *background checks*) anfordern: Pub. L. No. 92-544, 108 Stat. 1109, 1115 (1972).

460 *U. S. Department of Justice*, Attorney General's Report on Criminal History Background Checks, 2006, S. 3.

461 28 C. F. R. § 20.1 (2007).

Parlament jedoch eine Reihe von Gesetzen verabschiedet, die die Vertraulichkeit dieser Daten vermindern, indem sie die Hintergrundprüfungen für nicht strafrechtliche Zwecke nicht nur erlaubt, sondern auch beauftragt. Während der Kongress zuvor den Zugang zu den *criminal records* nur erlaubt hatte, begann er nunmehr, durch andere neue Rechtsvorschriften *background checks* sogar zu verlangen.[462] Nach den Terroranschlägen vom 11. September 2001 verabschiedete der Kongress mehrere Gesetze, die Hintergrundprüfungen für etwa eine Million Arbeiter fordern, einschließlich Gepäckprüfern, Hafen- und Chemiearbeitern, Beschäftigten in der Transportindustrie und des privaten Sicherheitspersonals und Personen, die bestimmte biologische Mittel behandeln. Diesbezüglich stellen die staatlichen Strafregister ihre Daten einigen Arbeitgebern und freiwilligen Vereinigungen zur Verfügung.[463] In diesem Zusammenhang stellen sich zwar viele Datenschutzfragen, in der vorliegenden Arbeit kann jedoch nicht konkret auf all diese Frage eingegangen werden; stattdessen beschränkt die Autorin sich auf die Datenschutzfrage bezüglich der Verwendung der Strafregistrierungen im Strafverfahren. Denn die *background checks* privater Unternehmen weichen vom Untersuchungsumfang der vorliegenden Arbeit ab.

Um einen unbefugten oder unverhältnismäßigen Zugriff auf Strafregistrierungen zu vermeiden, veranlassten mehr als die Hälfte der Bundesstaaten ihre Strafverfolgungsbehörden dazu, bei Datenanfragen Protokolle zu behalten, die die Benennung der Empfänger der *criminal history record information* und das Anfragedatum enthalten.[464] Einige Bundesstaaten stellen außerdem gewisse Ausbildungsanforderungen an das Personal, das an dem Eintragen von Daten in die *criminal history record systems* beteiligt ist. Die Tendenz geht dahin, einzelne personenbezogene Daten aus dem Strafregister leichter zugänglich zu machen. Die öffentliche Politik scheint darauf hinzuwirken, dass die Daten im Strafregister allgemein zugänglicher werden, sodass Behörden, Vereinigungen und Einzelpersonen, wenn

462 Zum Beispiel führten die Terroranschläge vom 11. September 2001 zu einer Gesetzgebung, die für Millionen Menschen die kriminalgeschichtlichen Hintergrundchecks fordert.

463 Siehe z. B. *U. S. Department of Justice*, Survey of State Criminal History Information Systems, 2003, Bureau of Justice Statistics, S. 8.

464 *Jacobs/Crepet*, The Expanding Scope, Use and Availability of Criminal Records, Legislation and Public Policy, Vol 11, 2008, 177, 57 f.

sie dies wollen, kriminalgeschichtliche Daten über beliebige Personen bei geschäftlichen und anderen Entscheidungen berücksichtigen können.[465]

Die datenschutzrechtliche Einschränkung der Auskunftserteilung aus dem Strafregister ist aus zwei Gründen weniger wirksam: den in Gerichten gespeicherten und von ihnen geführten Daten und der ansteigenden Anzahl privater Informationsvermittler mit eigenen Strafregisterdatenbanken. Ein großer Teil der *criminal history record information* über eine bestimmte Person ist öffentlich in *court dockets*[466] und *court records* zugänglich. Bis vor Kurzem waren jedoch die Strafregister einer Person nicht leicht abrufbar, da Suchende nicht Kenntnis darüber erlangen konnten, welche Gerichte die relevanten Daten besaßen. Die jüngste landesweite Zentralisierung und Automatisierung von Gerichtsaktensystemen haben die Identifizierung und Zugänglichkeit von Daten aber erheblich verbessert. Mit dem E-Government-Gesetz von 2002 wurde versucht, die Daten aus dem Strafregister über die Computersuche zugänglich zu machen.[467] Das Gesetz schreibt vor, dass Bundesbehörden und Bundesgerichte ihre Daten entweder per Fernzugriff oder alternativ durch Computerterminals vor Ort elektronisch zur Verfügung stellen.[468] Der zweite Grund für die weniger wirksame oder sogar unwirksame Einschränkung der Auskunftserteilung aus dem Strafregister liegt in der Existenz von sog. *criminal information brokers*. Nach dem ersten Verfassungszusatz kann niemand bestraft werden, wenn der Staat Daten an die Öffentlichkeit weitergibt.[469] Einige Unternehmen bauen ihre eigenen Datenbanken auf, indem sie in großen Mengen Strafregisterauszüge von Gerichten und staatlichen Strafregistern kaufen.[470,471] Sie entsenden in der Regel ihr Personal an die zuständigen

---

465 Es gibt zwar einige Einschränkungen, die sich jedoch darin erschöpfen, dass es Arbeitgebern verboten ist, Daten aus dem Strafregister in Arbeitsentscheidungen zu verwenden.

466 Ein *docket* enthält die Daten über Anklagen, Entscheidungen, Strafen und andere gerichtliche Ereignisse. Jedes Gericht verwaltet die Daten über jene Ereignisse (die *dockets* genannt werden), die vor dem jeweiligen Gericht stattgefunden haben.

467 Pub. L. No. 107-347. 116 Stat. 2889 (2002).

468 Pub. L. No. 107-347. 116 Stat. 2889 (2002), §§ 204–05.

469 *Solove/Schwartz*, Privacy Law: Fundamentals, S. 55: Der Staat kann aber die Daten nur unter der Bedingung zur Verfügung stellen, dass man zustimmt, deren Übermittlung einzuschränken.

470 *Jacobs/Crepet*, The Expanding Scope, Use and Availability of Criminal Records, Legislation and Public Policy, Vol 11, 2008, 177, 185 f.

471 In der Regel kommen die US-amerikanischen Gerichte zu dem Schluss, dass Informationen, die der Öffentlichkeit einmal zugänglich gemacht wurden, nicht

Gerichte in der Gegend, in der das Subjekt einer Hintergrundsuche gelebt hat, um die Strafregisterdaten über diese Person zu erhalten. Durch eine Internetsuche nach Strafregistern können die *criminal history records* den Privaten zur Überprüfungen der Beschäftigung oder der Wohnungsvermietung oder zu anderen Zwecken gegen eine geringe Gebühr übergeben werden. So erhöht sich das Bedürfnis nach Datenschutz durch eine einheitliche Regulierung der Strafregister immer weiter, weil die Daten, die von Gerichten oder von privaten Informationsanbietern in ihren Datenbanken geführt werden, der Öffentlichkeit leicht zugänglich gemacht werden.

4. Speicherdauer

Außer einiger Ausnahmevorschriften gibt es keine föderale Gesetzgebung, die zu einer allgemein verfügbaren Tilgung (*expungement*)[472] von Eintragungen im Strafregister ermächtigt. Die Speicherdauer ist also bundesgesetzlich nicht vorgesehen. Obwohl das Parlament keine föderale Begünstigungsgesetzgebung erlassen hat, die in den meisten Staaten zur Verfügung

---

mehr privat sein können. Zu einem anderen Verständnis der *privacy* siehe U. S. Department of Justice v. Reporters Committee for Freedom of the Press, 489 U. S. 749: Das Gericht stellt fest, dass es auch dann, wenn die Daten in einer öffentlichen Domain stehen, einen großen Unterschied zwischen öffentlichen Daten, die erst nach einer sorgfältigen Recherche der Gerichtsakten, Landesarchive und örtlichen Polizeibehörden im ganzen Land gefunden werden können, und einer computergestützten Zusammenfassung in einer Datenbank in einer einzigen Informationsstelle gibt. Dieses Verständnis von *privacy* unterscheidet sich stark von der Art und Weise, wie die meisten Gerichte *privacy* verstehen.

472 *Expungement* bedeutet wörtlich, dass eine Aufzeichnung oder ein Verfahren vollständig gelöscht wird und *sealing*, dass eine Aufzeichnung oder ein Verfahren „nur" versiegelt, aber nicht zerstört wird. In Bezug auf den Gebrauch in vielen staatlichen Gesetzen über die Behandlung strafrechtlich relevanter Daten werden die beiden Begriffe jedoch häufig synonym verwendet. *Expungement* wird im Sinn von *expunging* oder *sealing* einer Aufzeichnung oder *annulling* einer Verurteilung verwendet. Unabhängig vom verwendeten Begriff ist die Rechtsfolge im Allgemeinen dieselbe: Behördliche Daten, die einen strafgerichtlichen Fall identifizieren, werden für die Öffentlichkeit nicht zugänglich gemacht. Der Zugriff auf die Daten durch die Strafverfolgungsbehörden kann auch bei – nur in Bezug auf die Terminologie – getilgten Daten gesichert werden. Das Ausmaß, in dem die Daten tatsächlich vernichtet werden, ist unterschiedlich, aber typischerweise wird vom Strafjustizsystem ein Mindestmaß an Daten aufbewahrt.

stehen kann, und nicht einmal eine gesetzliche Speicherdauer existiert, können die Straftäter aufgrund bestimmter Gesetze ausnahmsweise unter bestimmten Umständen eine Tilgung genießen. Ein Beispiel dafür ist 18 U. S. C. § 3607 (c). Die Vorschrift sieht einen Umstand vor, in dem das Parlament der Judikative das Tilgungsermessen ausdrücklich erteilt.[473] Die Tilgungsermächtigung der Exekutive ist in 42 U. S. C. § 14132 (d) vorgeschrieben.[474] Außerdem wird der *Secretary of Veterans Affairs* dazu

---

473 18 U. S. C. § 3607 (c): "Expungement of Record of Disposition. – If the case against a person found guilty of an offense under section 404 of the Controlled Substances Act (21 U. S. C. § 844) is the subject of a disposition under subsection (a), and the person was less than twenty-one years old at the time of the offense, the court shall enter an expungement order upon the application of such person. The expungement order shall direct that there be expunged from all official records, except the nonpublic records referred to in subsection (b), all references to his arrest for the offense, the institution of criminal proceedings against him, and the results thereof. The effect of the order shall be to restore such person, in the contemplation of the law, to the status he occupied before such arrest or institution of criminal proceedings. A person concerning whom such an order has been entered shall not be held thereafter under any provision of law to be guilty of perjury, false swearing, or making a false statement by reason of his failure to recite or acknowledge such arrests or institution of criminal proceedings, or the results thereof, in response to an inquiry made of him for any purpose."

474 42 U. S. C. § 14132 (d): "Expungement of records –
(1) By Director
(A) The Director of the Federal Bureau of Investigation shall promptly expunge from the index described in subsection (a) the DNA analysis of a person included in the index—
(i) on the basis of conviction for a qualifying Federal offense or a qualifying District of Columbia offense (as determined under sections 14135a and 14135b of this title, respectively), if the Director receives, for each conviction of the person of a qualifying offense, a certified copy of a final court order establishing that such conviction has been overturned; or
(ii) on the basis of an arrest under the authority of the United States, if the Attorney General receives, for each charge against the person on the basis of which the analysis was or could have been included in the index, a certified copy of a final court order establishing that such charge has been dismissed or has resulted in an acquittal or that no charge was filed within the applicable time period.
(B) For purposes of subparagraph (A), the term "qualifying offense" means any of the following offenses:
(i) A qualifying Federal offense, as determined under section 14135a of this title.
(ii) A qualifying District of Columbia offense, as determined under section 14135b of this title.
(iii) A qualifying military offense, as determined under section 1565 of title 10.

ermächtigt, Daten über disziplinarische Angelegenheiten zu tilgen, die sich auf die beruflichen Verhaltensweisen oder Kompetenzen von *Veterans Health Administration*-Mitarbeitern beziehen.[475] Hierbei vertraten zahlreiche *Courts of Appeal* die Auffassung, dass es keine gerichtliche Befugnis gibt, Bundesstrafregistrierungen ohne eine bestimmte Gesetzgebung oder außerordentlich selten vorliegende und außergewöhnliche Umstände zu tilgen.[476] Die Bundesgerichte haben entschieden, dass die Tilgung dennoch aufgrund der einem Gericht innewohnenden Befugnisse oder vorbehaltlich der Ausübung der Nebenhoheit gewährt werden kann.[477] Aufgrund der Entscheidung des Supreme Courts im Jahr 1994, mit der die

---

(C) For purposes of subparagraph (A), a court order is not "final" if time remains for an appeal or application for discretionary review with respect to the order.
(2) By States
(A) As a condition of access to the index described in subsection (a), a State shall promptly expunge from that index the DNA analysis of a person included in the index by that State if—
(i) the responsible agency or official of that State receives, for each conviction of the person of an offense on the basis of which that analysis was or could have been included in the index, a certified copy of a final court order establishing that such conviction has been overturned; or
(ii) the person has not been convicted of an offense on the basis of which that analysis was or could have been included in the index, and the responsible agency or official of that State receives, for each charge against the person on the basis of which the analysis was or could have been included in the index, a certified copy of a final court order establishing that such charge has been dismissed or has resulted in an acquittal or that no charge was filed within the applicable time period.
(B) For purposes of subparagraph (A), a court order is not "final" if time remains for an appeal or application for discretionary review with respect to the order."

475 38 U. S. C. § 7462 (d) (1). "After resolving any question as to whether a matter involves professional conduct or competence, the Secretary shall cause to be executed the decision of the Disciplinary Appeals Board in a timely manner and in any event in not more than 90 days after the decision of the Board is received by the Secretary. Pursuant to the board's decision, the Secretary may order reinstatement, award back pay, and provide such other remedies as the board found appropriate relating directly to the proposed action, including expungement of records relating to the action."

476 Siehe auch *Mukherji*, In Search of Redemption: Expungement of Federal Criminal Records, S. 2.

477 Nur ein Bundesgericht stimmte zu, dass das Gesetz Bundesgerichte dazu befugt, Strafregistrierungen zu tilgen (United States v. Bohr, 406 F. Supp. S. 1218).

Nebenhoheit der Untergerichte begrenzt wurde,[478] sind die Circuit Courts in ihrer Ansichten darüber, ob die Tilgung nur aus gerechten Gründen in Betracht gezogen werden kann, gespalten. Der Supreme Court hatte inzwischen zwei Gelegenheiten, die Standpunktverschiedenheit der Circuit Courts zu lösen. Er hat sie jedoch nicht genutzt.[479]

Es herrscht jedenfalls Einigkeit darüber, dass auf der einzelstaatlichen Ebene keine gesetzliche Bestimmung über die bestimmte Speicherdauer von Strafregistrierungen existiert. Die *criminal history records* können jedoch auf staatlicher Ebene die Tilgung in irgendeiner Form genießen, obwohl die Gesetze je nach Einzelstaat unterschiedlich sind. In der Tat bietet jeder Staat unter bestimmten Umständen in irgendeiner Weise eine Form des *expungement*, wenn auch nur in begrenztem Ausmaß.[480] Insgesamt 36 Einzelstaaten gestatten es Einzelpersonen, dass ihre Strafverfahrensdaten ohne Verurteilung aus dem Strafregister gelöscht werden, wenn die Anklagen gegen sie fallengelassen oder sie im Strafverfahren freigesprochen wurden. Eine beträchtliche Anzahl von Einzelstaaten (24) sieht ferner die Löschung von Verurteilungen vor.[481] Die Strafverfahrensdaten ohne Verurteilungen allein haben ein beträchtliches Potenzial für nachteilige Folgen in den Bereichen der privaten Beschäftigung, der staatlichen Beschäftigung, der staatlichen Leistungen, der Zulassung zum Militär und des Erwerbs von Krediten. Ein ehemaliger Angeklagter verliert unter anderem seinen guten Ruf und hat Schwierigkeiten bei der Erlangung einer Anstellung, selbst wenn die Anklage fallen gelassen wurde. Eine Person, über die es Strafverfahrensdaten gibt, kann darüber hinaus Nachteile in verschiedenen weiteren Bereichen erfahren: die Vertreibung aufgrund einer Verhaftung vor einer Verurteilung oder die permanente Sperrung für den öffentlichen Wohnungsbau aufgrund einer Verurteilung;[482] Schwierigkeiten bei der Rückkehr in die Schule, als Konsequenz von *Federal Student Aid Ineligibi-*

478 Kokkonen v. Guardian Life Ins. Co. of Am., 511 U. S. 375 (1994).

479 Siehe *Mukherji*, In Search of Redemption: Expungement of Federal Criminal Records, 2013, S. 10 m. w. N (Rowlands v. United States, 127 S. Ct. 598 (2006) (cert. denied); United States v. Coloian, 128 S. Ct. 377 (2007) (cert. denied).

480 Wenn ein *criminal history record* versiegelt wird, hat die Öffentlichkeit keinen Zugang dazu, es sei denn, dass dies vom *district court* aus gutem Grund angeordnet wird. Bestimmte Strafjustizbehörden haben jedoch Zugang zu versiegelten Strafregistrierungen in ihrer Gesamtheit. Wenn die Daten demgegenüber getilgt werden, werden sie endgültig gelöscht.

481 *McAdoo*, Creating an expungement statute for the District of Columbia: A Report and Proposed Legislation, S. 1.

482 Department of Housing and Urban Development v. Rucker, 535 U. S. 125.

lity aufgrund bestimmter Verurteilungen;[483] ein lebenslanges Verbot von *Food Stamps* und *Temporary Assistance to Needy Families*;[484] Hindernisse für ein Familienleben wie ein Verbot von Pflege- und Adoptionsprogrammen.[485] Die Tilgung ist deshalb von Bedeutung, weil kollaterale Konsequenzen für die nicht gelöschten und damit ewig aufbewahrten Strafregistrierungen die Wiedereingliederung und die Rehabilitation von Straftätern (auch von ehemaligen Angeklagten) vereiteln und Rückfälligkeit fördern könnten.

Die Staaten haben unterschiedliche Mechanismen, um die Eintragungen in ihrem Strafregister zu tilgen. Zum Beispiel erlaubt der *California Penal Code* die Tilgungsbegünstigung von *Strafverfahrensdaten ohne Verurteilungen* für Verbrechen nur unter bestimmten Voraussetzungen: Wenn keine Anklage eingereicht wird, kann eine Person bei einer zuständigen Strafverfolgungsbehörde beantragen, ihre Daten löschen zu lassen. Die Behörde kann die Daten dieser Person nach der Feststellung der tatsächlichen Unschuld mit der Zustimmung der Staatsanwaltschaft versiegeln. Das Gleiche gilt, wenn ein Hauptverfahren eröffnet, aber der Angeklagte nicht verurteilt wurde. Das Gericht kann nach einem Freispruch auch von sich aus anordnen, die Daten zu versiegeln.[486] Maryland gewährt die Tilgung demgegenüber nicht nur bezüglich Strafverfahrensdaten ohne Verurteilungen, sondern auch bezüglich Verurteilungsdaten unter bestimmten anderen Voraussetzungen: bei allen Verbrechen außer Gewaltverbrechen, wenn die Verurteilung aufgehoben wird und wenn keine weiteren Verurteilungen (außer geringfügigen Verkehrsverstößen) oder anhängigen Verfahren vorliegen.[487] Die verschiedenen Elemente, die für eine Tilgungsentscheidung bedeutend sind – wie etwa Datenarten, Objektverbrechen, Wartezeiten bei einer entschiedenen Tilgung, die Möglichkeit von Rückfällen, die Beweislast und die Verwertungsmöglichkeit sowie das Schweigerecht des Betroffenen nach einer Begünstigung –, sind je nach Einzelstaat unterschiedlich geregelt. Dies ist besonders beunruhigend, da sich viele Staatsdelikte oder gleichwertige (d. h. ungeordnete) Straftaten mit Bundesdelikten überschneiden, und zahlreiche Verbrechen auf staatlicher Ebene haben fast identische föderale Gegenstücke, aufgrund derer Täter angeklagt werden können. Ob ein einmaliger minderjähriger Täter

483 20 U. S. C. 1091 (r).
484 21 U. S. C. 862a (a).
485 42 U. S. C. 671 (20) (a).
486 California Penal Code sec. 851.8.
487 Maryland Criminal Procedure Code Ann sec. 10-103.

oder ein Angeklagter, der sich als unschuldig erwiesen hat, dauerhaft mit dem Stigma einer Eintragung im Strafregister versehen wird, kann davon abhängen, wo er wegen der Straftat angeklagt wurde und ob er vor einem Einzelstaats- oder vor einem Bundesgericht angeklagt wurde.

Wird ein Blick auf die Tilgungsregelungen je nach Datenart auf einzelstaatlicher Ebene geworfen, kann Folgendes festgestellt werden: 26 Einzelstaaten erlauben die Tilgung von DNA-Daten nach einer Abweisung einer Verurteilung.[488] Jugendregistrierungen können in den meisten Staaten gelöscht werden, nachdem ein Minderjähriger das 18. oder das 21. Lebensjahr vollendet hat und die Person später nicht wegen eines anderen Verbrechens verurteilt wurde. Ein Verbrechen darf nur in einigen Staaten gelöscht werden. In den meisten Staaten können die Verhaftungsdaten, die nicht zu einer Verurteilung oder zu einer *guilty plea* führen, gelöscht werden, wenn für eine bestimmte Zeit keine weiteren Anklagen oder Verurteilungen vorliegen.[489] Die eine Tilgung ersuchende Person muss sich

---

488 ALA. CODE § 36-18-26 (2005); ARIZ. REV. STAT. § 13-610 (2004); CAL. PENAL CODE § 299 (Deering 2005); CONN. GEN. STAT. § 54-1021 (2004); DEL. CODE ANN. tit. 29, § 4713 (2005); GA. CODE ANN. § 24-4-65 (2004); IDAHO CODE § 19-5513 (Michie 2004); 730 ILL. COMP. STAT. § 5/5-4-3 (2005); IND. CODE ANN. § 10-13-6-18 (Michie 2004); KY. REV. STAT. ANN. § 17.175 (Michie 2004); LA. REV. STAT. ANN. § 15:614 (2004); ME. REV. STAT. ANN. tit. 25, § 1577 (2004); MASS. GEN. LAWS ch. 22E, § 15 (2004); MO. REV. STAT. § 650.055 (2004); MONT. CODE ANN. § 44-6-107 (2004); NEB. REV. STAT. § 29-4109 (2004); N.H. REV. STAT. ANN. § 651-C:5 (2004); N.J. REV. STAT. § 53:1-20.25 (2004); N.Y. [EXEC.] LAW § 995-c (Consol. 2005); N.C. GEN. STAT.§ 15A-148 (2004); N.D. CENT. CODE § 31-13-07 (2004); 44 PA. CONS. STAT. ANN.§ 2321 (West 2004); R.I. GEN. LAWS § 121.5-13 (2004); S.C. CODE ANN. § 23-3-660 (2004); S.D. CODIFIED LAWS § 23-5A-28 (Michie 2003); TEX. GOV'T CODE ANN. § 411.151 (Vernon 2004); VT. STAT. ANN. tit. 20 § 1940 (2004); VA. CODE ANN. § 19.2-310.7 (Michie 2004); W.V. CODE ANN. § 15-2B-11 (Michie 2005); WIS. STAT. ANN. § 165.77(4) (West 2004); WYO. STAT. ANN. § 7-19-405 (Michie 2004). Die Tilgung von DNA-Daten kommt meistens bei der Umkehrung von Verurteilungen, der fehlgeschlagenen Anklageerhebung und beim Ablehnungsbeschluss der Eröffnung des Hauptverfahrens aufgrund der Anklage vor.

489 ALASKA STAT. § 12.55.085 (Michie 2004) (conviction may be set aside if person was discharged by court without imposition of a sentence); ARK. CODE ANN. § 16-93-303 (Michie 2005) (first-time offender who completed probation, without a judgment of guilty, may have his record expunged); CAL. PENAL CODE § 851.85 (Deering 2005) (person acquitted of charge, if found factually innocent by the court, may have his records sealed); CONN. GEN. STAT. § 54-142a (2004) (person found not guilty of a charge, or if his charge is dismissed, may have his records erased upon expiration of time period for appeal);

in der Regel bei einer zuständigen Behörde melden und von sich aus Unterlagen zur Unterstützung der gewünschten Maßnahme vorlegen. In einigen Staaten muss eine Person, die eine Tilgung ersucht, die tatsächliche Unschuld beweisen.[490] Nebraska verlangt, dass Einzelpersonen durch klare und überzeugende Beweise zeigen, dass sie versehentlich verhaftet wurden,

---

DEL. CODE ANN. tit. 10, § 1025 (2005) (person may request expungement of criminal records if charge is dismissed or not otherwise prosecuted); GA. CODE ANN. § 353-37 (2004) (person arrested for an offense but not prosecuted, or if charges are dismissed, may request expungement of records); 20 ILL. COMP. STAT. § 2630/5 (2005) (person acquitted or released without being convicted may request expungement of records upon showing good cause); IND. CODE ANN. § 35-38-5-1 (Michie 2004) (person may request expungement of arrest record if no charges filed, charges dropped due to mistake, no offense was committed, or upon an absence of probable cause); KAN. STAT. ANN. § 22-2410 (2005) (person may request expungement of arrest record); KY. REV. STAT. ANN. § 431.076 (Michie 2004) (person charged but found not guilty, or against whom charges were dismissed, may request expungement of all records, including arrest records, fingerprints, photographs and other data); MD. CODE ANN. [CRIM. PROC.] § 10-103 (LexisNexis 2004) (person may request expungement of arrest record if no charges filed); MISS. CODE ANN. § 99-15-57 (2004 (records shall be expunged if case dismissed or otherwise not prosecuted); N.J. REV. STAT. § 2C:52-6 (2004) (if arrest does not result in conviction, record may be expunged); N.C. GEN. STAT. § 15A-146 (2004) (arrest that does not result in conviction may be expunged); OHIO REV. STAT. ANN. § 2953.52 (Anderson 2005) (person may request sealing of records anytime after found not guilty or charges dismissed, or after two years from the return of no bill by a grand jury); OKLA. STAT. tit. 22 § 18 (2004) (person arrested with no charges filed, or upon reversal of conviction, may request expungement); 18 PA. CONS. STAT. ANN. § 9122 (arrest records expunged after eighteen months from date of arrest upon order or certification of no proceedings); S.C. CODE ANN. § 17-1-40 (2004) (arrest records expunged if acquitted or charges dismissed); TENN. CODE ANN. § 40-32-101 (2004) (expungement of arrest records available at no cost if acquitted, charges dismissed, arrested without charges, or no bill returned by a grand jury); UTAH CODE ANN. §§ 77-18-9 – 15 (2005) (expungement of arrest records available if released without charges filed, charges dismissed or acquitted); VA. CODE ANN. § 19.2-392.2 (Michie 2004) (person may request expungement if charged and acquitted, pardoned, or charges dismissed); W. V. CODE ANN. § 61-11-25 (Michie 2005) (person found not guilty or charged dismissed may apply for expungement of arrest records if no previous felony convictions); WYO. STAT. ANN. § 7-13-1401 (Michie 2004) (person may request expungement if at least 180 days since arrested and no charges filed or charges dismissed).

490 *Diehm*, Federal Expungement: A Concept in Need of a Definition, St. John's Law Review, Vol 66. No. 1, 1992, 73, 74.

um ihre Verhaftungsdaten löschen zu lassen.[491] Im Gegensatz dazu hält Maine die Informationen automatisch geheim, wenn keine Verurteilung erfolgt.[492]

Die Löschung von Verurteilungsdaten wird in der Regel dem Ermessen des Gerichts überlassen, wenn der Angeklagte nicht innerhalb einer bestimmten Frist weitere Verurteilungen erhält, nachdem er aus der Haft oder aus der Bewährung entlassen wurde. Fast jedes Gericht erlaubt die Tilgungsbegünstigung für ein erstmaliges Vergehen, insbesondere wenn es von einem Minderjährigen begangen wurde, solange über einen bestimmten Zeitraum hinweg – in der Regel zwei bis fünf Jahre – keine weiteren Verurteilungen vorliegen.[493] Verurteilungen, die rückgängig gemacht oder abgelehnt wurden, werden auf Anfrage oft gelöscht. Darauf muss der Angeklagte jedoch je nach Schwere des Verbrechens zwischen einem und zehn Jahren warten.[494] Die Verhaftungsdaten können in den meisten Staaten gelöscht werden, wenn sie nicht zu einer Verurteilung führten.[495] Die Löschung der Strafregistrierungen bezüglich sexueller Verbrechen ist hingegen meistens nicht möglich. Dies erlauben nur einige Staaten unter bestimmten Umständen.[496] Die Tilgung der Sexualstrafregistrierungen gestaltet sich deshalb schwierig oder ist sogar unmöglich, weil Sexualstraftä-

491 NEB. REV. STAT. § 29-3523 (2004) (person may have erroneous arrest record expunged upon showing of clear and convincing evidence).

492 ME. REV. STAT. ANN. tit. 16, § 613 (2004).

493 KY. REV. STAT. ANN. § 431.078 (Michie 2004) (person convicted of a misdemeanor or other minor violation may request expungement after five years); MISS. CODE ANN. § 99-15-59 (2004) (first-time misdemeanor offender may have conviction expunged).

494 N. H. REV. STAT. ANN. § 651.5 (2004).

495 Der Zugang zu den gelöschten Daten durch öffentliche Behörden wird in Nebraska aber außerordentlich gesichert: NEB. REV. STAT. § 29-3523 (2004) („Arrest records may be sealed, except for public officials or candidates for public office, if prosecution is inactive or completed within one year").

496 In Idaho können Sexualstraftäter nach zehn Jahren eine Tilgung ihrer Strafregistrierungen und die Befreiung von ihrer Pflicht zur Registrierung in der staatlichen Datenbank beantragen, wenn sie durch eindeutige und überzeugende Nachweise belegen, dass sie nicht in Gefahr sind, erneut straffällig zu werden, und dass keine ähnlichen Anklagen anhängig sind. Für Sexualverbrechen der Personen, die wegen einer schweren Straftat verurteilt wurden, ist keine Tilgung möglich. In ähnlicher Weise können Sexualstraftäter in Nebraska eine Tilgung beantragen, wenn sie nicht mehr dazu verpflichtet sind, sich in der staatlichen Datenbank anzumelden, wenn sie durch eindeutige und überzeugende Beweise nachweisen können, dass ihnen kein Risiko einer Rückfälligkeit droht und dass keine ähnlichen Anklagen erhoben werden. Zur lebenslangen Registrierung in der staatlichen Datenbank verurteilte Straftäter können ihre

ter einem höheren Rückfallrisiko ausgesetzt sind als diejenigen, die andere Straftaten begehen, und weil die Gesellschaft Sexualstraftaten für besonders abscheulich hält. Die Staaten erlauben daher für Sexualdeliktsdaten keine Löschungsbegünstigung, selbst wenn keine Verurteilung vorliegt. Der Grund hierfür könnte darin liegen, dass die Staaten die Daten für mögliche zukünftige, damit verbundene Anklagen gegen denselben Straftäter behalten wollen. Eine solch rigorose Haltung gegenüber bestimmten Verbrechen kann zudem bei häuslicher Gewalt[497] festgestellt werden. An die Tilgung von Strafregistrierungen im Zusammenhang mit häuslicher Gewalt werden tendenziell strengere Anforderungen gestellt als an die Tilgung üblicher Verbrechen; die Tilgung ist hier im Allgemeinen aber leichter als bei Sexualstraftaten.[498]

Die Tilgung scheint dennoch höchst problematisch zu sein, nicht nur wegen ihrer begrenzten Natur, sondern auch wegen Schwierigkeiten in der Durchsetzung. Aufgrund des Systems, in dem die Daten von Gerichten geführt werden und für die Öffentlichkeit leicht zugänglich sind, und wegen der starken Verbreitung kommerzieller Informationsanbieter mit eigenen Strafregisterdatenbanken wird das einheitliche Datenmanagement schwierig. Denn es ist schwer sicherzustellen, dass die unter bestimmten Umständen schon gelöschten Datensätze vollständig, also aus allen Datenbanken gelöscht werden. Auch wenn die Tilgungsvorschrift auf staatlicher Ebene getroffen wurde, liegt das Problem darin, alle in verschiedenen Systemen gespeicherten Daten effektiv zu verwalten oder die Wirksamkeit des Informationsmanagements zu gewährleisten, da es kompliziert ist, die Strafregisterdatenbank der privaten Informationsvermittler gesetzlich einzuschränken.

Außerdem scheinen die versiegelten Daten im Strafregister dafür, dass sichergestellt wird, dass sie später, möglicherweise gemäß einer gerichtlichen Anordnung, geöffnet werden können, zwar praktischer zu sein,

---

Daten nicht löschen lassen (*McAdoo*, Creating an Expungement Statute for the District of Columbia: a Report and Proposed Legislation, S. 8).

497 Der Begriff der häuslichen Gewalt umfasst den Kindesmissbrauch, den Ehegattenmissbrauch und den Missbrauch von abhängigen Erwachsenen.

498 Vgl. N. Y. [FAM. CT. ACT] § 1051 (2005); ALA. CODE § 26-14-3 (2005); ARK. CODE ANN. § 5-28-220 (Michie 2005); COLO. REV. STAT. § 19-3-505 (2004); GA. CODE ANN. § 49-5-184 (2004); HAW. REV. STAT. ANN. § 350-2 (Michie 2004); IDAHO CODE § 39-5304 (Michie 2004); 325 ILL. COMP. STAT. § 5/7.14 (2005); ME. REV. STAT. ANN. tit. 22, § 4008 (2004); S.C. CODE ANN. § 22-5-910 (2004); R.I. GEN. LAWS § 12-1-12 (2004); S.D. CODIFIED LAWS § 26-8A-11 (Michie 2003); VT. STAT. ANN. tit. 33 § 4916 (2004).

unterliegen jedoch dem erheblichen Risiko einer absichtlichen oder versehentlichen Offenlegung. Vor dem Aufkommen des Internets konnten die Daten vielleicht erfolgreich versiegelt werden. Unter den Bedingungen der modernen Informationsverarbeitung ist eine wirksame Versiegelung jedoch weniger wahrscheinlich. Sobald bestimmte Daten für einen bestimmten Zeitraum auf einer Webseite veröffentlicht werden, können diese öffentlich verbreiteten Daten nicht mehr effektiv geheim gehalten oder vertraulich behandelt werden. Die staatliche Registerbehörde wird bei der Verwaltung ihrer Ver- oder Entsiegelungsaufgaben auf Schwierigkeiten stoßen. Zudem bleibt die Frage, ob die Arbeitgeber nach versiegelten Strafregistrierungen fragen können, und wenn sie es tun, ob eine Person, deren Daten in einem Strafregister versiegelt wurden, die Tatsache wahrheitsgemäß beantworten muss,[499,500] weil die Tilgung oder die Versiegelung gesetzlich nicht mit einem sogenannten Verwertungsverbot verbunden ist.

Neben der vielfältigen Art und den wachsenden Volumina der *criminal history records* hat sich auch der Zugang zu diesen dramatisch erweitert. Nicht nur die fortgeschrittene Informationstechnik und die zunehmende Rolle der Strafregistereintragungen im Strafverfahren, sondern auch die einzelstaatlich ermächtigten, vom Parlament zugelassenen oder sogar beauftragten *criminal background checks*, die Entstehung der blühenden Privatwirtschaft, die den *criminal background checking service* für Kunden bietet, die aggressive Übermittlung der *criminal records* für Sexualstraftäter infolge der Verbreitung der Megans Gesetze drängen darauf, angemessene Schutzmaßnahmen für hochsensible Daten einzuführen. In den USA scheint das Bewusstsein für den Schutz personenbezogener Daten im Strafverfahren aber noch unzureichend zu sein. Angesichts dessen sollten vermehrt politische Überlegungen über den effektiven und angemessenen Datenschutz im Strafverfahren angestellt werden.

---

499 *Jacobs*, Mass Incarceration and the Proliferation of Criminal Records, Vol. 3 Issue 3, Univ. Of St. Thomas Law Journal, S. 412.

500 Insgesamt 28 Staaten erlauben es Einzelpersonen, deren Eintragungen im Strafregister gelöscht wurden, die ehemalige Existenz solcher Daten zu verschweigen, wenn sie danach gefragt werden. Dies geschieht dadurch, dass eine *Legal Fiction* geschaffen wird, die notwendig ist, um den Zweck der Tilgung zu verfolgen und die Personen von der Stigmatisierung und den lebenslangen kollateralen Konsequenzen solcher Daten zu befreien (*Mukherji*, In Search of Redemption: Expungement of Federal Criminal Records, S. 36 m. w. N.).

II. Rasterfahndung

Nach der deutschen Rechtsordnung ist eine Rasterfahndung ein maschineller Abgleich von Daten, die sowohl bei öffentlichen als auch bei privaten Stellen gespeichert sind, um bestimmte Verdächtige festzustellen oder Nichtverdächtige auszuschließen. Der Datenabgleich, der einer Rasterfahndung im Sinne von § 98a in der deutschen StPO funktional vergleichbar ist, wird in den USA unter dem Namen des *Computer Matching* reguliert und verwendet. Seitdem das *Computer Matching* in den frühen 1970er Jahren möglich wurde, wird es heute insbesondere in der Regierungsverwaltung häufig verwendet, vorwiegend, um Gesetzesverstöße im Zusammenhang mit dem Empfang staatlicher Leistungen zu ermitteln. Der Computer Matching and Privacy Act von 1988[501] hat den Privacy Act von 1974 geändert, indem bestimmte Schutzbestimmungen für diejenigen Personen hinzugefügt wurden, deren Datensätze in den automatisierten Matching-Programmen verwendet werden. Das Gesetz schränkt die *Computer Matching*-Programme nicht ein, sondern legt nur Verfahren für Bundesbehörden fest, die sich mit dem *Computer Matching* der Daten befassen.[502] Die Verfahrensregelungen gelten nur für den Datenabgleich von Daten, die bei öffentlichen Stellen gespeichert sind, aber nicht für den Abgleich, der Datenbestände verwendet, die im Besitz Privater sind. Das beruht in den US-amerikanischen Datenschutzgesetzen vor allem auf dem Fehlen eines Konzepts, das der Idee des grundgesetzlichen Verbots mit Erlaubnisvorbehalt entspricht. Denn jede Datenverarbeitung ist in den USA grundsätzlich zulässig, sofern es keine speziellen Bestimmungen gibt, die dagegen sprechen,[503] während die Datenverarbeitung in Deutschland nur auf Basis eines Erlaubnistatbestandes zulässig ist. Die Erhebung und der Abgleich von Daten, die sich im Besitz Privater befinden, werden somit grundsätzlich gesetzlich nicht geregelt. Die gesetzliche Regelung betrifft angesichts der Gefahren staatlicher automatisierter Datenverarbeitung nur den Abgleich von Daten, die bereits bei einer Behörde gespeichert sind. Das *Computer Matching*, das dem Computer Matching and Privacy Act von 1988 unterliegt, ist also ein computergestützter Abgleich maschinen-

501 Computer Matching and Privacy Protection Act of 1988, P. L. 100–503.

502 *Solove/Schwartz*, Privacy Law: Fundamentals, S. 67.

503 Zum Beispiel der Social Security Act (42 U. S. C. § 1320b-7), der Tax Reform Act aus dem Jahr 1976 (Public Law 94–455, Department of Defense Authorization Act of 1983, Public Law 97–252) usw. Die meisten speziellen Gesetze ermächtigen aber nur dazu, einen Abgleich durchzuführen, enthalten jedoch keine weiteren Einzelheiten für die Durchführung der Maßnahme.

lesbarer Datensätze, die nur bei öffentlichen Stellen bereits gespeicherte personenbezogene Daten von vielen Personen enthalten, um Missbrauch staatlicher Leistungen festzustellen.[504] Für die Verwendung der bei einer Bundesbehörde gespeicherten Daten von einer anderen Behörde zum Zweck eines Datenabgleichs wird eine Datenübermittlung von einer Behörde zu der anderen Behörde vorausgesetzt. Dabei ist der Privacy Act von 1974 einschlägig, der allgemeine datenschutzrechtliche Bestimmungen für alle bei Bundesbehörden gespeicherten Daten enthält. Das Gesetz umfasst aber nicht den Abgleich, der bei einer privaten Stelle gespeicherte Daten verwendet.

Gegen das *Computer Matching* werden verfassungsrechtliche Bedenken erhoben, da hierfür kein Tatverdacht erforderlich ist, obwohl polizeiliche Untersuchungen nach den Grundsätzen des vierten Verfassungszusatzes und dem im fünften und sechsten Verfassungszusatz verankerten Prinzip der Unschuldsvermutung normalerweise nur beim Vorliegen eines Tatverdachts zulässig sind. Auch der Umfang der Untersuchungen, bei denen alle Personen in den betroffenen Dateien als mögliche Täter angesehen werden, ist Gegenstand von Kritik.[505] Mit der Entwicklung der Computertechnologie ist nicht nur die Fähigkeit entstanden, große Mengen an Daten zu speichern, sondern auch die Fähigkeit, Daten automatisch zu sortieren, zu extrahieren und abzugleichen. Die Bedenken hinsichtlich des Datenabgleichs werden dann besonders akut, wenn die Regierung viele sensible Daten auf einer einzigen Datenbank besitzt oder besitzen kann.

Nachfolgend soll deshalb zum einen gesondert den Rechtsgrundlagen für den Abgleich nachgegangen werden, der bereits bei öffentlichen Stellen gespeicherte Datenbestände verwendet, und zum anderen auch der Abgleich untersucht werden, der Datenbestände im Besitz Privater verwendet. Anschließend soll durch die Analyse gesetzlich getroffener spezifischer Absicherungsvorkehrungen untersucht werden, ob das Dateninteresse oder die Freiheitsrechte des Einzelnen beim Abgleich sowohl bei öffentlichen als auch bei nicht öffentlichen Stellen gespeicherter Daten entsprechend der Eingriffsintensität der Maßnahme geschützt werden.

504 5 U. S. C. § 552a (a) (8) (A).

505 *Lützner*, USA, in: *Gropp* (Hrsg.), Besondere Ermittlungsmaßnahmen zur Bekämpfung der Organisierten Kriminalität, S. 763 und m. w. N.

1. Organisationsstruktur

a) Datenübermittlung als Vorbedingung eines Datenabgleichs

aa) Überblick

Ein maschineller Datenabgleich besteht vor allem aus der Datenübermittlung von einer Speicherstelle als Voraussetzung eines Abgleichs und dem automatisierten Datenabgleich als dem endgültigen Ziel. Die Einschränkung der Datenübermittlung wirkt unterschiedlich, je nachdem, wo die Daten gespeichert sind, also in den Speichersystemen der Bundesbehörden, der einzelstaatlichen Behörden oder eines privaten Unternehmens. Die Einschränkung eines maschinellen Datenabgleichs gilt nur für den Datenabgleich durch die Bundesbehörden. Wie oben erwähnt, ist in den USA grundsätzlich jede Datenverarbeitung zulässig, sofern es keine speziellen Bestimmungen gibt, die dagegen sprechen. Eine Datenübermittlung und ein computergestützter Datenabgleich sind daher ohne anderslautende Vorschriften grundsätzlich zulässig und werden in den USA nur im Bereich eines Datenabgleichs durch die Bundesbehörden geregelt.

bb) Unterschiedliche Regulierung der Übermittlung der öffentlichen und privaten Daten

Auf Bundesebene sind mehrere Gesetze im Hinblick auf den behördlichen Datenabgleich in Kraft getreten.[506] Diese Gesetze legen wichtige Grundprinzipien für das behördenübergreifende Datenmanagement auf allen Regierungsebenen fest. Das erste Bundesgesetz, das auf den Schutz des Interesses bezüglich der *data privacy* abzielte, war der Privacy Act von 1974, der unter anderem ein Verbot der behördenübergreifenden Offenlegung personenbezogener Daten ohne Zustimmung der betroffenen Person vorsah.[507] Danach dürfen die Behörden nur jene Daten über eine Person speichern und verwalten, die zu einem Zweck, der gesetzlich oder auf Anordnung des Präsidenten zu erfüllen ist, relevant und notwendig sind (5 U. S. C. § 552a (e) (1)). Eine Datenübermittlung zum Zweck eines Datenabgleichs ist grundsätzlich an eine Zustimmung der Betroffenen

506 So der Tax Reform Act of 1976, Public Law 94-455, Department of Defense Authorization Act of 1983, Public Law 97-252.

507 5 U. S. C. § 552a (b).

gebunden. Die Datenübermittlung ist also in der Regel nur dann zulässig, wenn die Datenübermittlung an eine Person oder eine andere Behörde von den Betroffenen schriftlich angefragt oder wenn ihr vorher schriftlich zugestimmt wird. Das Gesetz umfasst keinen Datenabgleich *nach* einer eingeleiteten spezifischen strafrechtlichen oder zivilrechtlichen Ermittlung einer oder mehrerer bestimmter Personen, um Beweise gegen diese Personen zu erheben. Die Auslegung des Wortlauts der Norm spricht dafür, dass die Norm nur auf das *Data Matching* angewendet wird, das zur Identifizierung einiger Verdächtigen *vor* dem Beginn einer konkreten strafrechtlichen Untersuchung durchgeführt wird.

Der Computer Matching and Privacy Protection Act von 1988, ein Änderungsgesetz des Privacy Act, sieht die Regulierung des Datenabgleichs der Bundesregierung vor.[508] Die Gesetzgebung ist zustande gekommen, weil der Privacy Act von 1974 nach der Ansicht des Kongresses für Personen, deren Daten zum Datenabgleich verwendet werden mussten, wenig Schutz bot.[509] Das Gesetz enthält explizitere Richtlinien, die regeln, wie Daten zwischen Regierungsbehörden ausgetauscht werden und inwieweit die Behörden auf der Grundlage von übermittelten und dann ausgeglichenen Daten nachteilige Maßnahmen gegen Einzelpersonen treffen dürfen. Außerdem legt das Gesetz die Standards für das ordnungsgemäße Verfahren fest, die das Ausmaß beschränken, in dem die Behörden auf der Grundlage abgeglichener Daten handeln können. Es sieht vor, dass zwischen Behörden keine Daten ausgetauscht werden dürfen, es sei denn, dies ist unter bestimmten Voraussetzungen schriftlich vereinbart (5 U. S. C. § 552a (o) (1)). Datenabgleichvorgänge unterliegen aber nicht immer, sondern nur in bestimmten Fällen diesem Gesetz. Es ist z. B. dann nicht einschlägig, wenn ein *Matching* im Anschluss an die Einleitung einer bestimmten strafrechtlichen oder zivilrechtlichen Untersuchung gegen eine oder mehrere bekannte Personen von einer Behörde (oder einem Teil davon) durchgeführt wird, die jegliche Tätigkeit im Zusammenhang mit der Durchsetzung des Strafgesetzes als ihre Hauptaufgabe führt, um Beweise gegen diese Person oder diese Personen zu sammeln.[510] Die Auslegung des Wortlauts der Norm spricht dafür, dass die Norm nur auf das *Data*

508 Mit dem Computer Matching and Privacy Protection Act (CMPPA) von 1988 ist der Schutz durch den Privacy Act auf das *matching program* ausgedehnt.

509 Siehe Committee on Government Operations, Computer Matching and Privacy Protection Act of 1988, H.R. Rep. No. 100–802, 100th Cong., 2d Sess. 3107, 1988 (3114).

510 5 U. S. C. § 552a (a) (8) (B) (iii).

Matching angewendet wird, das zur Identifizierung einiger Verdächtigen *vor* dem Beginn einer konkreten strafrechtlichen Untersuchung durchgeführt wird.

Beim EDV-Abgleich, der Datenbestände im Besitz Privater verwendet, verhält sich dies anders. Dieser Unterschied beruht auf der Tatsache, dass im Privacy Act die Unterstützungspflicht einer Speicherstelle, die keine öffentliche Stelle ist, nicht berücksichtigt wird und es im Privatsektor so gut wie keine datenschutzrechtlichen Regelungen gibt.[511] Die datenschutzrechtlichen Belange wurden hier nur in einigen Industriezweigen gesetzlich geregelt, etwa im Finanzsektor, in der Telekommunikationsindustrie, im Hochschulbereich und in der Fernsehindustrie. Unter diesen Bedingungen verfügen die Ermittlungsbehörden über eine Reihe von Instrumenten, um auf die Daten des Privatsektors zugreifen zu können; dies sind zum einen die unverbindlichen und zum anderen die verbindlichen Möglichkeiten. Die Ermittlungsbehörden können Daten unverbindlich auf dem Datenmarkt entgeltlich erwerben. In vielen Staaten verkauft beispielsweise das Verkehrsamt Listen von Führerschein- und Autoinhabern, die unter anderem Geburtsdaten und die gefahrenen Automarken enthalten. Dies beruht auf der Verkürzung des Schutzes der begründeten Erwartung auf *privacy* durch die *third party doctrine*. Dabei können Daten, die einmal an Dritte weitergegeben wurden, keinen Schutz mehr genießen.[512] Können Daten nicht entgeltlich erworben werden, hängt der Zugang der Ermittlungsbehörde zu Daten von der Kooperationsbereitschaft der jeweiligen Datenbesitzer ab. Viele Datenbesitzer wollen Daten für polizeiliche Ermittlungszwecke ohne Vorlage einer *subpoena* oder einer anderen vergleichbaren gerichtlichen Anordnung aber nicht herausgeben.[513] Ohne

511 *Lützner*, USA, in: *Gropp* (Hrsg.), Besondere Ermittlungsmaßnahmen zur Bekämpfung der Organisierten Kriminalität, S. 759 und m. w. N.: „Als Begründung wird angeführt, dass die unterschiedliche Größe und Belange der verschiedenen Industriezweige einen Ausgleich zwischen dem Datenschutz und den legitimen Interessen Dritter an bestimmten Daten in einem einzelnen Gesetz nicht ermögliche."

512 Smith v. Maryland, 442 U. S. 735 (1979); Couch v. United States, 409 U. S. 322 (1973); United States v. Miller, 425 U. S. 435 (1976). Die unteren Gerichte haben die *third party doctrine* in großem Umfang angewandt, etwa auf die Daten über die Internetnutzung einer Person, die durch ISPs gespeichert sind: United States v. Forrester, 512 F. 3d 500 (9th Cir. 2008); Guest v. Leis, 255 F. 3d 325 (6th Cir. 2001).

513 In einer umfassenden Umfrage der University of Illinois über den Umgang mit Daten bei den größten amerikanischen Firmen erklärten 62 Prozent der Befragten, dass Daten nur gegen Vorlage einer *subpoena* einer staatlichen Stelle

subpoena o. Ä. ist also kaum zu erwarten, dass die privaten Datenbesitzer der Strafverfolgungsbehörde willig ihre Daten weiterleiten und den Datenabgleich unterstützen. Der Staat verfügt außerdem über eine Reihe von verbindlichen Instrumenten, um auf die Daten des privaten Sektors zuzugreifen: Gesetze mit Meldepflichten (z. B. der Bank Secrecy Act), *National Security Letters* (NSLs) oder *subpoena* bzw. eine gerichtliche Anordnung. Der Bank Secrecy Act schreibt die Aufbewahrung von Bankunterlagen und die Erstellung von Berichten vor, die für strafrechtliche, steuerliche oder behördliche Ermittlungen oder Verfahren nützlich sind. Erforderlich ist, dass die bundesweit versicherten Banken die Identität der Kontoinhaber sowie Kopien jedes Schecks, Wechsels oder sonstigen Finanzinstruments speichern müssen (12 U. S. C. § 1829b). Viele Bundesdatenschutzgesetze sehen den behördlichen Zugang zu privaten Daten durch eine gerichtliche Anordnung oder *subpoena* vor, die die lockeren Standards für den Zugang zu Daten enthalten, also weniger strikt als *probable cause* sind. Ein Beispiel hierfür ist der Right to Financial Privacy Act (REPA),[514] der vorschreibt, dass die Finanzdaten einer Person nur aufgrund einer *subpoena* oder eines Durchsuchungsbefehls an die staatlichen Behörden weitergegeben werden dürfen. Die *National Security Letters*[515] sind ein weiterer Mechanismus, mit dem die Behörden Daten aus dem privaten Sektor erhalten können. Damit darf das FBI die Vorlage von Daten verlangen, wenn dies für das Sammeln ausländischer Geheimdienste oder eine Terrorismusermittlung von Belang ist. Eine weitere Zugriffsermächtigung des FBI kommt aus den PATRIOT Act *§ 215 Orders*. Diese Vorschriften aus dem PATRIOT Act erlauben es

---

zugänglich gemacht werden. Hierzu ausführlich *Linowes*, Privacy in America: Is Your Private Life in the Public Eye? Urbana [u. a.], Univ. of Illinois Press, 1989, S. 44.

514 Der Right to Financial Privacy Act von 1978, Pub. L. 95 – 630, 29 U. S. C. §§ 3407. Weitere Gesetze, die von den staatlichen Behörden verlangen, eine gerichtliche Anordnung oder *subpoena* zu erhalten, um auf private Daten zuzugreifen, sind z. B. der Cable Communications Policy Act (CCPA), 47 U. S. C. § 551 (h), der Fair Credit Report Act (FCRA), 15 U. S. C. § 1681 f, der Health Insurance Portability and Accountability Act (HIPAA), 45 C. F. R. § 164.512 (f) (1), der Pen Register Act, 18 U. S. C. § 3123(a), der Stored Communications Act (SCA), 18 U. S. C. § 2703 und der Video Privacy Protection Act (VPPA), 18 U. S. C. § 2710 (b) (2) (C).

515 Die National Security Letters (NSLs) sind ein außergewöhnliches Durchsuchungsverfahren, mit dem das FBI die Offenlegung von Kundendaten erzwingen kann, die Banken, Telefongesellschaften, Internet Service Provider und andere bewahren. Zum Beispiel der Stored Communications Act, 18 U. S. C. § 2709; der Right to Financial Privacy Act, 12 U. S. C. § 3414 (a) (5) (A); der Fair Credit Reporting Act, 15 U. S. C. § 1671u.

dem FBI, die Vorlage von materiellen Gegenständen für Ermittlungen zum Schutz gegen internationalen Terrorismus oder Geheimdienstaktivitäten anzuordnen, es sei denn, dass solche Ermittlungen gegen US-amerikanische Bürger ausschließlich auf der Grundlage von Aktivitäten durchgeführt werden, die durch den ersten Verfassungszusatz geschützt werden. Ein Antrag auf eine *Section 215 Order* ist an einen Richter zu richten und es ist anzugeben, dass die Daten für eine befugte Ermittlung eingeholt werden sollen.

Daten, die von Behörden gespeichert oder privat aufbewahrt werden, können, wie oben erklärt, zum Zweck des Datenabgleichs auf unterschiedliche Weise an die Ermittlungsbehörden übermittelt werden. Die übermittelten Daten bilden eine Vorbedingung eines maschinellen Datenabgleichs.

b) Funktionsweise des Datenabgleichs

Der Computer Matching and Privacy Protection Act (CMPPA) begründet die Verfahren für den maschinellen Datenabgleich durch die Bundesbehörden. Das Gesetz schränkt die *matching programs* nicht ein, sondern fordert von den Behörden, die Verfahren zu veröffentlichen und die Betroffenen vor dem Abgleich zu benachrichtigen. Behörden, die einen maschinellen Datenabgleich vornehmen wollen, müssen außerdem ein *data integrity board* einrichten und eine Genehmigung vom *board* erhalten. Dabei kommt es nicht darauf an, ob die Daten bei den öffentlichen Behörden oder bei Privaten gespeichert sind. Wenn die Daten zum maschinellen Datenabgleich an die Bundesbehörden übermittelt werden, gilt dafür das CMPPA. Das Gesetz erfordert eine Benachrichtigung vor dem einzelnen Datenabgleich, um das Recht der Betroffenen zu schützen.

Die auf diese Weise übermittelten Daten werden folgenderweise abgeglichen:

(1) Von jeder Datenbank, die als Quelle für das Datenabgleichprogramm verwendet wird, werden alle verfügbaren Datenelemente aus allen verfügbaren Datensätzen ausgewählt. (2) Gegebenenfalls finden Datenbereinigungsoperationen statt, damit die Organisation, das Format und der Inhalt einer oder mehrerer Dateien in eine für den Abgleichsschritt geeignete Form geändert werden. (3) Danach wird ein Matching durchgeführt, wobei auf die Dateien mit personenbezogenen Daten ein Matching-Algorithmus angewendet wird, um Treffer zu finden. Damit sind übereinstimmende Datensätze gemeint, die sich auf dieselbe Person beziehen. (4)

Es kommt dann zu einer Inferenz, bei der eine Inferenzprozedur auf das Ergebnis des Abgleichprozesses angewendet wird (d. h. entweder auf den Inhalt von übereinstimmenden Datensatzpaaren oder auf das Vorhandensein oder Nichtvorhandensein von Übereinstimmungen). Der Zweck dieses Schritts ist es, Rückschlüsse auf die Person zu erhalten, auf die sich die Daten beziehen, oder auf ihr Verhalten, ihre Handlungen oder Neigungen. (5) Treffer werden in diesem Schritt gefiltert, um einen effizienten Einsatz von Ermittlungsressourcen zu gewährleisten und ungerechtfertigte Verwaltungsmaßnahmen zu vermeiden. (6) Auf Grundlage der Analyse von resultierenden Informationen werden Entscheidungen getroffen und Maßnahmen ergriffen. (7) Gegebenenfalls werden neue Datensätze erstellt oder die bestehenden Datensätze geändert oder erweitert. (8) Eine Qualitätsanalyse kann auf allen Stufen ein Feedback generieren, das eine Rückkehr zu früheren Schritten erfordert.[516]

2. Abgleichbare Daten

5 U. S. C. § 552a (a) (4) erwähnt als für einen Abgleich verfügbare Daten alle Artikel, Sammlungen oder Gruppierungen von Informationen über eine Person, die von einer Behörde geführt werden, einschließlich – aber nicht darauf beschränkt – ihrer Ausbildung, Finanztransaktionen, der medizinischen Vorgeschichte, der Straf- oder Beschäftigungsgeschichte, und Daten, die den Namen der Person oder die identifizierende Nummer, das Symbol oder ein anderes identifizierendes Merkmal enthalten, das der Person zugewiesen werden kann, wie etwa ein Finger- oder Stimmabdruck oder ein Foto. Die Vorschrift sieht also keine Beschränkungen für bestimmte personenbezogene Daten vor, die zum Abgleich verwendet werden dürfen. Es gibt viele Möglichkeiten, wie Daten in den Besitz einer Behörde gelangen können: Sie können von der Behörde erstellt werden oder durch Beobachtung der betroffenen Person oder ihres Verhaltens oder als Nebenprodukt einer Transaktion zwischen der Behörde und der betroffenen Person erstellt werden. Die Behörde kann die Daten auch von der betroffenen Person selbst, von einer anderen Behörde oder erneut von einer Behörde erwerben, an die sie weitergegeben wurden.[517] All

516 *Clarke*, Dataveillance by Governments: The Technique of Computer Matching, Information Technology & People, Vol. 7 No. 2, 1994, 46.

517 *Clarke*, A Normative Regulatory Framework for Computer Matching, Vol. 13 Issue 4, Journal of Computer & Information Law, 1995, S. 598.

die Daten, die bei der Behörde auf verschiedene Weisen erworben oder erstellt und dann gespeichert wurden, können der Gegenstand eines Datenabgleichs sein.

Auch im Falle von Daten im Privatbesitz kann eine Behörde alle personenbezogenen Daten ohne Beschränkung erwerben und sie zum Abgleich verwenden, solange die Datenbesitzer zur Herausgabe von Daten für polizeiliche Ermittlungszwecke bereit sind.

3. Verwendung des Datenabgleichs

Der Privacy Act macht es von der Zustimmung der Betroffenen abhängig, ob Daten, die für einen bestimmten Zweck erhoben wurden, später für einen anderen Zweck verwendet werden dürfen. Grundsätzlich darf keine Behörde ohne Zustimmung des Betroffenen ihre Daten zur Durchführung eines Abgleichs an eine andere Stelle weiterleiten. Ungeachtet dieser Bestimmung kommt der Zustimmung des Betroffenen eine schwache Bedeutung zu. Denn im Falle eines Datentransfers zwischen Behörden derselben Regierungsebene (z. B. zwischen US-Bundesbehörden oder zwischen den Behörden eines bestimmten Staates) nehmen es Regierungsbehörden manchmal zum Vorwand, dass sie Mitglieder eines monolithischen öffentlichen Dienstes sind. Dadurch können sie behaupten, dass alle Datenübertragungen zwischen Regierungsstellen interne und nicht externe Übertragungen sind.[518] Solche totalitären Tendenzen können den Schutz des Rechts auf informationelle Selbstbestimmung mit der Kontrolle durch die verfahrensrechtlichen Vorkehrungen entmachten. Ein weiterer Faktor, der die Zustimmung der betroffenen Personen bedeutungslos macht, ist die

518 *Clarke*, Computer Matching and Digital Identity, 1993: Um dieses Problem in den Griff zu bekommen, sagt Clarke, der Gesetzgeber müsse unbedingt klarstellen, dass Behörden für die Zwecke der Datenübertragung unabhängige Organisationen sind, damit alle Datenübertragungen den Regeln für die Sammlung und Verbreitung unterliegen. Außerdem betont er eine umfassende und universell anwendbare Datenschutzgesetzgebung, die ein ausgewogenes Verhältnis zwischen den verschiedenen wirtschaftlichen und sozialen Interessen erreicht, und er fordert die Errichtung einer Kontrollstelle, die über ausreichende Befugnisse und Ressourcen verfügt, um ein angemessenes Gleichgewicht zwischen der informationellen Privatsphäre und der administrativen Effizienz zu erreichen (*Clarke*, A Normative Regulatory Framework for Computer Matching, Vol. 13 Issue 4, Journal of Computer & Information Law, 1995, S. 611 ff.; zustimmend zur Idee der Einrichtung einer solchen Stelle siehe auch *Laudon*, Computers and Bureaucratic Reform, S. 384).

Ausnahmemöglichkeit unter Verwendung des Begriffs „routine use“[519]. Der Privacy Act lässt die Ausnahmemöglichkeit offen und der Ausnahmetatbestand wird in der Praxis großzügig ausgelegt. Ein Problem liegt also darin, dass viele Abgleichvorgänge im Rahmen des *routine use*-Ausnahmetatbestandes durchgeführt werden. Ein Datenabgleich wird in der Praxis oft einfach als *routine use* von Daten betrachtet. Infolgedessen sind Behörden in der Lage, die Anforderung des Privacy Act zu umgehen, dass Einzelne der Verwendung ihrer Daten für einen anderen als den ursprünglich vorgesehenen Zweck zustimmen müssen. Der Privacy Act sieht vor, dass das *Computer Matching* durchgeführt werden kann, um die Berechtigung oder die fortwährende Einhaltung gesetzlicher oder aufsichtsrechtlicher Anforderungen von Bewerbern, Empfängern oder Begünstigten von oder Teilnehmern an der Erbringung von Dienstleistungen in Bezug auf Geld- oder Sachleistungen oder Zahlungen im Rahmen von Bundesleistungsprogrammen festzustellen oder zu überprüfen, um Zahlungen zurückzuzahlen oder Schulden im Rahmen solcher Bundesleistungsprogramme zu tilgen. Der Hauptanwendungsbereich dieser Maßnahme war bis dato die Identifizierung solcher Personen, die unberechtigt staatliche Leistungen empfangen oder beantragt haben. Die Bedeutung des Verwendungszwecks des Datenabgleichs ist aber gering, weil das *Computer Matching* häufig als Routinemaßnahme durchgeführt wird. Das Gesetz wird aufgrund eines Defekts der großzügigen Auslegung der Ausnahmetatbestände als ein „Papiertiger“ angesehen.[520] Darüber hinaus ist eine Zustimmung der Betroffenen sogar dann nicht erforderlich, wenn eine Strafverfolgungsbehörde eine schriftliche Anfrage an eine Behörde gerichtet hat, die die Daten führt, und in dieser schriftlichen Anfrage der gewünschte Teil dieser Daten und der Zweck angegeben ist, für den die Daten angefragt werden.[521]

Der Computer Matching and Privacy Protection Act von 1988 sieht zusätzliche Verfahren vor, schafft jedoch keine inhaltlichen Leitlinien, um zu bestimmen, wann ein Abgleich akzeptabel ist. Er legt Entscheidungen über einen Datenabgleich in die Hände einzelner Verwaltungsbehörden, die verpflichtet sind, bestimmte Verfahren zu befolgen. Die Durchführung eines Datenabgleichs ist beispielsweise verboten, wenn keine schriftliche

519 5 U. S. C. § 552a (a) (7): *Routine use* bedeutet die Weiterverwendung von erhobenen Daten, wenn die spätere Verwendung mit dem Erhebungszweck vergleichbar ist.

520 Siehe *Carlson/Miller*, Public Data and Personal Privacy, Santa Clara High Technology Law Journal, Vol. 16 Issue 1, 2000, S. 105.

521 5 U. S. C. § 552a (b) (7).

Vereinbarung zwischen der Speicherstelle und der Anfragestelle getroffen wurde. Eine behördenübergreifende Datenübermittlung zum Zweck eines Datenabgleichs ist also nur nach schriftlicher Vereinbarung zwischen der Speicherstelle und der Anfragestelle möglich. Denn das Gesetz sieht vor, dass Daten zwischen Behörden nicht ausgetauscht werden dürfen, es sei denn, dies ist unter bestimmten Voraussetzungen schriftlich vereinbart. Die Matching-Vereinbarungen müssen den Zweck des geplanten Datenabgleichs festlegen, die Datensätze beschreiben, die abgeglichen werden, und Verfahren zur Benachrichtigung über unerwünschte Ereignisse auf der Grundlage eines Datenabgleichs festlegen.[522]

4. Aufbewahrungsdauer der Daten

Trotz Bemühungen auf Bundesebene, die mit dem Datenabgleich verbundenen Privacy-Interessen zu berücksichtigen, gibt es keine Bestimmungen, die Aufbewahrungsdauer für die Ergebnisse eines Datenabgleichs mit sowohl bei öffentlichen als auch bei privaten Stellen gespeicherten Daten zu beschränken. Die Aufbewahrungsdauer der Daten hängt also nur von der schriftlichen Vereinbarung ab, aufgrund derer die Behörden Daten austauschen können.[523] Nach 5 U. S. C. § 552a (o) (1) (I) soll die schriftliche Vereinbarung Verfahren für die Rückgabe der Datensätze an die Speicherstelle oder die Vernichtung von Datensätzen enthalten, die in einem Datenabgleich verwendet werden. Bestimmte Aufbewahrungsfristen, Rückgabezeiten von Daten an eine Speicherstelle oder Löschungs- oder Vernichtungszeiten nach einem Abgleich sind nicht gesetzlich festgelegt. Dies gilt auch für den Abgleich der Daten, die auf dem Datenmarkt entgeltlich gekauft oder von einer privaten Stelle aufgrund einer *subpoena* oder einer gerichtlichen Anordnung erhalten wurden. In diesem Fall ist nicht einmal eine schriftliche Vereinbarung erforderlich.

Es gibt zwar keine Löschungsregelungen für die Daten, die in den Speichersystemen privater Unternehmen gespeichert sind, aber zahlreiche Bundesstaaten haben Gesetze, nach denen ein Unternehmen personenbe-

522 Zu den Einzelheiten der sog. *matching agreements* 5 U. S. C. § 552a (o) (1).

523 Aufgrund dieser fehlenden externen Kontrolle über das *Computer Matching* argumentiert *Laudon*, dass eine Datenschutzgesetzgebung der zweiten Generation erforderlich sei (*Laudon*, Computers and Bureaucratic Reform, S. 400).

zogene Daten sicher und effektiv vernichten muss, wenn es die Daten nicht mehr speichern will.[524]

5. Mitteilungspflicht

Die *vor* dem Abgleich erforderlichen Verfahren werden durch wichtige Schutzmaßnahmen für die Bürger *nach* dem Datenabgleich flankiert. Die notwendigen Schutzmaßnahmen sind in 5 U. S. C. (p) geregelt. Die erste Maßnahme betrifft die Frage, inwieweit eine unabhängige Überprüfung der in einem Abgleich verwendeten personenbezogenen Daten erforderlich ist, bevor die Behörde Maßnahmen in Bezug auf die Person ergreift. Verlangt wird entweder, (1) dass ein Beamter der Behörde eine unabhängige Überprüfung der Daten bezüglich nachteiliger Maßnahmen gegen jede Person unternimmt, deren Daten in *matching programs* verwendet werden, oder (2) dass die Daten auf die Identifizierung und die Höhe der Leistungen beschränkt sind, die von einer Speicherstelle im Rahmen eines staatlichen Leistungsprogramms gezahlt werden, und dass ein hohes Maß an Vertrauen besteht, dass die der Anfragestelle zur Verfügung gestellten Daten zutreffend sind.[525] Der Privacy Act verlangt, dass die Betroffenen eine Mitteilung von der Behörde erhalten, die eine Erklärung ihrer Ergebnisse beinhaltet, und dass sie über die Möglichkeit informiert werden, solche Feststellungen anzufechten. Personen müssen nach dem Gesetz also benachrichtigt werden, wenn Leistungen aufgrund von übereinstimmenden Daten reduziert oder gekündigt werden sollen, und sie können eine Frist von dreißig Tagen haben, um die Ergebnisse anzufechten. Der Computer Matching Act verpflichtet die Behörden dazu, die Benachrichtigungsme-

524 Alaska Stat. § 45.48.500; Ariz. Rev. Stat. § 44-7601; Ark. Code Ann. § 4-110-104; Cal. Civ. Code § 1798.81; Colo. Rev. Stat. § 6-1-713; Conn. Gen. Stat. Ann. § 42-471; Ga. Code § 10-15-2; Haw. Rev. Stat. § 487R-2; 20 ILCS 450/20; Ind. Code §§ 24-4-14-8 und 24-4.9-3-3.5(c); Kan. Stat. Ann. § 50-7a03; Ky. Rev. Stat. § 365.725; Mass. Gen. Laws Ch. 931, § 2; Md. Code, Comm. Law § 14-3507; MCL § 445.72a; Mo. Stat. § 288.360; Mont. Code Ann. § 30-14-1703; Nev. Rev. Stat. § 603A.200; N.J. Stat. § 56:8-162; N.Y. Gen. Bus. Law § 399-H; N.C. Gen. Stat. § 75-64; Ore. Rev. Stat. § 646A.622; R.I. Gen. Laws § 6-52-2; S.C. Code § 37-20-190; Tex. Bus. & Com. Code. Ann. § 72.004; Utah Code Ann. § 13-44-201; 9 Vt. Stat. Ann. § 2445; Wash. Rev. Code § 19.215.020; Wisc. Stat. § 134.97.

525 5 U. S. C. 552a (p) (1) (A). Die zweite Alternative schwächt die Erfordernis einer unabhängigen Verifizierung durch die Forderung nach der generellen Genauigkeit der Daten.

thode der betroffenen Personen in der Vereinbarung anzugeben. Obwohl der Computer Matching Act keine inhaltlichen Anforderungen für die Entscheidung enthält, wann ein Datenabgleich angemessen ist, bietet er einige Verfahrensschutzmaßnahmen für den Einzelnen, einschließlich dieser Möglichkeit, nach dem Datenabgleich der Genauigkeit der Ergebnisse zu widersprechen. Die Benachrichtigungspflicht an Einzelpersonen ist aber nicht mit einem Datenabgleich als solchem, sondern mit den nachteiligen Maßnahmen aufgrund von Ergebnissen eines Datenabgleichs verbunden. Wird also keine nachteilige Maßnahme getroffen, findet auch keine Benachrichtigung statt.

Eine Bundesbehörde darf zur Durchführung eines Abgleichs grundsätzlich nur mit der Zustimmung des Betroffenen dessen Daten an eine andere Stelle weiterleiten. Dass die Bedeutung dieser Beschränkungsvorschrift wegen der großzügigen Auslegung der Ausnahmetatbestände verlorengegangen ist, wurde oben bereits dargelegt. Die spezifische Kontrolle, die der Computer Matching Act zum Datenschutz eines Einzelnen vorsieht, erfolgt in zwei Richtungen: zum einen als Information an den Kongress, zum anderen als die Einrichtung eines Datenaufsichtsausschusses innerhalb einer den Datenabgleich vornehmenden Behörde. Eine Kopie der Vereinbarung, die alle beteiligten Behörden vor der Durchführung des Abgleichs treffen müssen, ist dreißig Tage vor Beginn der Maßnahme an einen Ausschuss des Kongresses zu schicken (5 U.S.C. § 552a (o) (2)). Daneben sieht das Gesetz bei allen am *Computer Matching* beteiligten Behörden die Einrichtung eines Datenaufsichtsausschusses vor, der bei allen Abgleichvorgängen die Einhaltung der gesetzlichen Vorgaben überwachen soll. Ein Datenaufsichtsausschuss muss innerhalb jeder Behörde eingerichtet werden, bevor diese an Matching-Vereinbarungen teilnehmen kann (5 U. S. C. 552a (u)). Der Datenaufsichtsausschuss überwacht und koordiniert unter den verschiedenen Abteilungen einer solchen Behörde die Implementierung dieser Vorschrift durch die Behörde. Er ist dazu verpflichtet, jährlich einen Bericht zu erstellen und diesen dem Leiter der Behörde sowie dem *Office of Management and Budget* vorzulegen.

III. Vorratsdatenspeicherung

1. Geschichtlicher Hintergrund

Das Freiheits- und Persönlichkeitsinteresse der Bürger muss gegen die Verantwortung des Staates abgewogen werden, seine Bürger vor ausländi-

schen Bedrohungen zu schützen, Verbrechen zu ermitteln und das geltende Recht durchzusetzen. Dies ist deshalb nicht einfach, weil im digitalen Zeitalter neue Herausforderungen entstehen, denen mit konventionellen Mitteln schwer oder gar nicht begegnet werden kann. Eines der neuen Ermittlungsmittel ist die Vorratsdatenspeicherung. Hierbei handelt es sich um ein kriminalpolitisches Instrument, das die Kommunikationsdienstanbieter dazu verpflichtet, bestimmte Daten zum Zweck einer eventuellen Ermittlung, Feststellung und Verfolgung bestimmter Straftaten vorrätig und anlasslos zur Verfügung zu stellen. In den USA existiert aber keine Bestimmung, die die Telekommunikationsunternehmen zur vorrätigen und anlasslosen Speicherung bestimmter Daten verpflichtet, obwohl mehr als zwanzig Jahre lang eine ähnliche Praxis herrschte, ohne dass die Bevölkerung davon wusste. Diesbezüglich wurde in den USA im Jahr 2013 durch Snowdens Enthüllungen ein Skandal verursacht. Der Skandal führte dazu, dass die Bevölkerung über die Datenspeicherungspraxis des Staates informiert wurde. An diesem erstaunlichen Ereignis sind die mehrfachen Versuche des Parlaments, die Vorratsdatenspeicherung einzuführen, gescheitert. Der Gesetzgebungsfehlschlag gründet sich nicht nur auf der geschichtlichen Erfahrung der Bevölkerung in Verbindung mit einer Reihe von Ereignissen bezüglich der Metadatensammlung des Staates, sondern auch unmittelbar auf das fehlende Datenschutzgesetz: Es gibt in den USA so gut wie keine Datenschutzgesetze im Privatsektor. Die privaten Unternehmen können deshalb nach Belieben und ohne weitere Einschränkungen Daten speichern. In dieser Situation sorgt sich der Staat bei einer Anforderung der Daten wenig darum, dass die Daten zum Anfragezeitpunkt im Unternehmen verlorengehen und deshalb nicht mehr gespeichert sind.

In diesem Zusammenhang wurden die sog. Quick-Freeze-Verfahren unter dem ECPA (Electronic Communications Privacy Act von 1986)[526] ohne eine Vorratsdatenspeicherung implementiert. Hierbei ist eine anlassbezogene Speicherung der bei den Telekommunikationsunternehmen vorhandenen Daten vorgesehen („einfrieren"). Bei Verdachtsfällen kommt es auf Anordnung der Strafverfolgungsbehörden zu einer „vorübergehenden Sicherung" der Daten. Unter bestimmten Voraussetzungen können diese eingefrorenen Daten den Ermittlungsbehörden zur Verfügung gestellt werden („auftauen"). Der Zugriff auf die Daten ist damit möglich. Im Folgenden soll zuerst der historische Hintergrund näher erläutert werden, der dazu geführt hat, dass die US-amerikanische Datenspeicherungspraxis

526 ECPA Pub. L. 99-508, Oct. 21, 1986, 100 Stat. 1848, 18 U. S. C § 2510.

sich auf das Quick-Freeze-Verfahren beschränkt; danach soll die aktuelle Datenspeicherung unter dem Quick-Freeze-Verfahren untersucht werden.

a) Die Datensammlung der DEA als eine Vorlage für die Metadatensammlung der NSA

Die Antidrogenbehörde DEA (*Drug Enforcement Administration*) hat zwanzig Jahre lang Milliarden von Telefonverbindungsdaten mit noch weniger demokratischer Kontrolle gespeichert. Die DEA betrieb eine riesige Datenbank mit Telefonverbindungsdaten namens USTO.[527] Anstatt die Telefongesellschaften um Anrufdaten von Personen zu ersuchen, die wegen Drogenverbrechen verdächtig wurden, hatte das Justizministerium Telefonanbietern die Anordnung erteilt, Listen aller Anrufe aus den USA in Länder zu übertragen, in denen nach Ansicht der Regierung Drogenhändler operieren. Die Behörde leitete Informationen von Geheimdienstabhörungen, Informanten und der Datenbank mit Telefonverbindungsdaten an Behörden im ganzen Land weiter, um ihnen dabei zu helfen, strafrechtliche Ermittlungen gegen Amerikaner einzuleiten.[528] Die DEA erhielt die Daten mit administrativen *subpoenas*, die es der Behörde erlaubten, Daten zu sammeln, die für Bundesdrogenuntersuchungen relevant oder wesentlich sind. Es handelte sich zwar um eine weite Auslegung dieser Befugnis, die jedoch wahrscheinlich nicht angefochten wird, da die *subpoenas* im Gegensatz zu Durchsuchungsbefehlen keiner gerichtlichen Anordnung bedürfen.

Um das Programm geheim zu halten, wurden die Verbindungsdaten nie als Beweismittel in Prozessen oder als Grundlage für Durchsuchungsbefehle verwendet. Die Anfangsdaten, die aus den oben erwähnten Quellen stammen, wurden effektiv an einem zentralen Ort der SOD (*Special Operation Division*) bereinigt, bevor sie an Mitarbeiter von Behörden einschließlich der DEA, des *Internal Revenue Service*, des FBI und der *Homeland*

527 In der DEA-Datenbank namens USTO wurden unabhängig davon, ob gegen die Beteiligten ein Verdacht vorlag, Verbindungsdaten zu Gesprächen ins Ausland gespeichert: Die Telefonnummern sämtlicher US-Bürger, die irgendwann einmal in eines von 116 Ländern telefonierten, werden mitsamt der Nummer des Angerufenen, der Uhrzeit und der Gesprächsdauer gespeichert.

528 *Shiffman/Cooke*, Exclusive: U. S. directs agents to cover up program used to investigate Americans, REUTERS v. 5.8.2013, abrufbar unter: https://www.reuters.com/article/us-dea-sod/exclusive-u-s-directs-agents-to-cover-up-program-used-to-investigate-americans-idUSBRE97409R.

Security gesendet wurden. Eine Ermittlungsbehörde erhielt von der SOD einen Geheimtipp, nach dem die Anfangsdaten aus der ursprünglichen Quelle nicht als Beweismittel verwendet wurden, führte dann eine separate Untersuchung durch und konstruiert daraus die unabhängigen, im Prozess anzuerkennenden Beweise. Die Methode wird als *parallel construction* bezeichnet. Die *parallel construction* wurde wegen Verstoßes gegen die verfassungsmäßigen Rechte der jeweils Angeklagten auf ein faires Verfahren und wegen der vorgerichtlichen Entdeckungsregelung kritisiert, damit Beweise unterschlagen werden, die sich für die jeweils Angeklagten als nützlich erweisen könnten.[529]

Das USTO-Programm wurde erst nach den Snowden-Enthüllungen im Mai 2013 eingestellt. Seitdem übergab die DEA den Mobilfunkbetreibern jeden Tag eine Liste mit Telefonnummern, deren Anschlussinhaber sie verdächtigte, und verlangte die entsprechenden Verbindungsdaten. Die inzwischen eingestellte Operation, die von der DEA durchgeführt wurde, war die erste bekannte Bemühung der Regierung, Verbindungsdaten von Millionen US-Bürgern in Massen zu sammeln, unabhängig davon, ob sie einer Straftat verdächtigt wurden oder nicht. Es war ein Modell für das massive Telefonüberwachungssystem, das die NSA nach den Anschlägen vom 11. September 2001 einsetzte, um Terroristen zu identifizieren.

b) Metadatensammlung[530] der NSA

aa) Die Anschläge vom 11. September 2001 als Wendepunkt

Ein Großteil dessen, was über das Massenmetadatensammlungsprogramm der NSA bekannt ist, stammt aus Dokumenten, die durch die Snowden-Offenlegung veröffentlicht wurden. Die Praxis der Metadatensammlung der NSA vor den Anschlägen am 11. September 2001 ist daher kaum bekannt.

---

529 *Shiffman/Cooke*, Exclusive: U. S. directs agents to cover up program used to investigate Americans, REUTERS v. 5.8.2013, abrufbar unter: https://www.reuters.com/article/us-dea-sod/exclusive-u-s-directs-agents-to-cover-up-program-used-to-investigate-americans-idUSBRE97409R.

530 Metadaten enthalten Informationen zu einem Anruf – wer, wo, wann und wie lang –, aber nicht den Inhalt der Kommunikation.

Die NSA ist gemäß der *executive order* 12333[531] dazu ermächtigt, die Daten ausländischer elektronischer Nachrichtendienste zu sammeln und zu analysieren und die Sicherheit von geheimen US-Computersystemen zu gewährleisten.[532] Die Befugnisse der NSA wurden aber während eines verdeckten Programms von 1956 bis 1971 missbraucht, als die Behörde die Geheimdienstdaten sammelte und verschiedene US-Bürger überwachte.[533] Als Reaktion auf den Missbrauch wurde der Foreign Intelligence Surveillance Act (FISA) erlassen, dessen Ziel die Begrenzung der Massenüberwachung in den USA ist. Gemeinsam mit dem FISA wurde auch der *Foreign Intelligence Surveillance Court* (FISC oder FISA-Court) eingerichtet, dessen Aufgabe es ist, die FISA-Anordnungsanträge zu überprüfen.[534] Die FISA-Anordnungsanträge müssen hinreichend wahrscheinlich (*probable cause*) sein, damit zu der Annahme gelangt werden kann, dass „das Ziel der elektronischen Überwachung eine ausländische Macht oder ein Vertreter einer ausländischen Macht ist"[535] und dass sich die gesuchten Informationen auf die nationale Sicherheit beziehen. Bei einer FISA-Anordnung ist, anders als bei der Title-III[536], kein *probable cause* für die Annahme erforderlich, dass die Zielperson ein Verbrechen begangen hat oder begehen wird.

---

531 Executive Order No. 12,333, 3 C. F. R. 1981, available at http://www.archives.gov/federal-register/codification/executive-order/12333.html. Department of Defense Personnel Security Program Regulation, 3 C. F. R. 1981, 32 C. F. R. § 154 (2012). "The collection of foreign intelligence or counterintelligence within the United States shall be coordinated with the FBI as required by procedures agreed upon by the Director of Central Intelligence and the Attorney General." a. a. O. Siehe 1.8. "Agencies with the Intelligence Community are authorized to collect, retain, or disseminate information concerning United States persons only in accordance with procedures established by the head of the agency concerned and approved by the Attorney General." a. a. O., siehe 2.3.

532 *Ahuja*, FAQ: What you need to know about NSA surveillance and Edward Snowden, WASHINGTON POST v. 5.8.2013, abrufbar unter: https://www.propublica.org/article/nsa-data-collection-faq.

533 NAT'L COMM'N TERRORIST ATTACKS UPON THE UNITED STATES, 9/11 COMMISSION REPORT 75 (July 22, 2004) [hereinafter 9/11 COMMISSION REPORT], available at http://www.9-llcommission.gov/report/9llReport.pdf; *Baker*, In the Common Defense, 2014.

534 *Baker*, In the Common Defense, 2014, S. 79–80.

535 50 U. S. C. § 1804 (a) (4) (A) (2014).

536 Title-III ist eine Abhörmaßnahme des Bundes und ein Verweis auf den Teil des Omnibus Crime Control and Safe Streets Act von 1968 Pub. L. No. 90–351, 82 Stat. 197 (codified as amended in scattered sections of 42 U. S. C.), der die Strafverfolgungsbehörden dazu ermächtigte, die Erlaubnis zum Abhören von kabelgebundenen und mündlichen Kommunikationen ohne das Wissen oder die Zustimmung der Teilnehmer zu beantragen. 18 U. S. C. § 2518 (2000 &

Unter den FISA-Anforderungen können Ausländer auch ohne eine gerichtliche Anordnung überwacht werden, soweit es *keine substanzielle Wahrscheinlichkeit* dafür gibt, dass die Überwachung den Inhalt einer Kommunikation offenlegt, an der US-Bürger teilnehmen.[537] Der Großteil der von der NSA durchgeführten Überwachung fällt unter die Kategorie „Ausländer zu Ausländer" und wird daher von der FISA nicht erfasst, da die Überwachung in Übersee und in der Regel gegen Ausländer erfolgt.

Früher gab es bei der Übermittlung der von der NSA gespeicherten Daten eine Mauer zwischen der Strafverfolgungsbehörde und dem Geheimdienst, die verhinderte, dass eine Strafverfolgungsbehörde die FISA-Daten verwendet, um die Notwendigkeit einer rechtmäßigen Titel-III-Anordnung zu negieren und die Anforderung absichtlich zu umgehen, einen *probable cause* für eine Entscheidung darüber zu entwickeln, ob eine Zielperson eine Straftat schon begangen hat oder begehen wird. Hier wurde ein Verfahren über die Übermittlung und die Weitergabe der von der NSA gespeicherten Daten eingerichtet. Die Mauer konnte nur mit der Zustimmung des Generalstaatsanwalts und des FISC überwunden werden. So gab es keinen Grund zur Sorge, dass die Geheimdienstdaten in einem Strafverfahren gegen einen Angeklagten verwendet würden.

Nach den Anschlägen vom 11. September 2001 wurde die Befugnis der NSA, nationale Kommunikationen zu überwachen, zuerst durch das *President's Surveillance Program* (PSP) und später durch gesetzliche Grundlagen – den PATRIOT Act[538] – erweitert. Mit dem PATRIOT Act von 2001 wurden die Exekutivbefugnisse auch in der Telekommunikationsüberwachung

---

Supp. 2014) legt die verfahrensrechtlichen Anforderungen an die Überwachung fest. Das Gesetz regelt im Wesentlichen Folgendes: (1) Es verbietet der Regierung, eine unbefugte und nicht einvernehmliche Überwachung der Kommunikation per Telefon, Internet, E-Mail usw. zu implementieren; (2) es legt das Verfahren fest, wie die Regierung eine gerichtliche Anordnung zur Durchführung einer Abhörmaßnahme anfordern kann; und (3) es regelt die Offenbarung von abgefangenen Kommunikationen. Um eine gerichtliche Anordnung für das Abhören kabelgebundener oder elektronischer Kommunikationen zu erhalten, muss ein föderales Verbrechen begangen werden und die Identität der Zielpersonen, ihr kriminelles Verhalten und die Art und Weise, in der das Zielgerät zur Förderung der Strafverfolgung verwendet wird, müssen angegeben werden. Es wird manchmal gesagt, dass die Titel-III-Anordnungen schwieriger zu erhalten sind als die FISA-Anordnung.

537 50 U. S. C. § 1802 (B).

538 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism (der USA PATRIOT Act) Act of 2001, sec. 208 (1), Pub. L. No. 107-56, 115 Stat. 272 [im Folgenden: der PATRIOT Act] (codified in scattered titles of U.S.C.), at sec. 203. Den PATRIOT Act verabschie-

umfangreich erweitert, damit die Daten für die Ermittlung, Feststellung und Verfolgung schwerer Straftaten zur Verfügung stehen. Die Erweiterung des Zugriffs der Strafverfolgungsbehörden zu den elektronischen Daten erfolgte mit der Reduktion der Data Privacy der Bürger. Der PATRIOT Act erlaubte zum einen, dass Telekommunikationsunternehmen unter bestimmten Bedingungen die Kommunikations- und Standortdaten an die Strafverfolgungsbehörden freiwillig übergeben, und erweiterte zum anderen die Arten von Daten, die den Strafverfolgungsbehörden mit *subpoenas* verfügbar sind.

Die Gesetze durchbrachen unter dem Abschnitt 203 mit dem Titel *Authority to share criminal investigative information* vor allem die Mauer, die den Datenaustausch zwischen Nachrichtendienst- und Strafverfolgungsbehörden blockiert hatte. Der Abschnitt 215 des PATRIOT Act ermächtigte die Regierung außerdem dazu, eine geheime gerichtliche Anordnung zu beantragen, mit der Dritte wie Telefongesellschaften dazu aufgefordert werden können, Daten oder andere „tangible things" zu übergeben, wenn sie für eine Untersuchung relevant sind, die der Sammlung ausländischer nachrichtendienstlicher Daten, die nicht US-Bürger betreffen, oder dem Schutz vor internationalem Terrorismus oder Geheimdienstaktivitäten dient. Aber die Regierung glaubte immer noch, dass sie aufgrund der Third-Party-Doktrin[539] nicht einmal gerichtliche Anordnungen benötigt, wenn sie beschließt, diese Daten mit *subpoenas* zu sammeln. Auf dieser Grundlage hat die NSA von Telekommunikationsanbietern Listen mit allen von ihren Kunden geführten und erhaltenen Anrufen angefordert und erhalten, einschließlich der üblicherweise aufgezeichneten Metadaten wie Uhrzeit, Dauer des Anrufs und Telefonnummern am Endgerät (aber nicht

---

dete der Kongress am 25. Oktober 2001 als Reaktion auf die Anschläge vom 11. September 2001.

539 Die *Fourth Amendment* verbietet nicht den Erhalt von Daten, die Dritten gegenüber offengelegt und von diesen an Regierungsbehörden übermittelt wurden, auch wenn die Informationen in der Annahme offenbart werden, dass sie nur für einen begrenzten Zweck verwendet werden und das Vertrauen in Dritte nicht verraten wird (United States v. Miller, 425 U. S. 435 (1976), S. 443). Im Anschluss an Miller entschied der Gerichtshof in der Entscheidung Smith v. Maryland, dass ein Anrufer keine begründete Erwartung auf *privacy* hat, wenn er seine Daten freiwillig an Telefongesellschaften weitergibt. Das beruht auf der Erwägung, dass der Anrufer bei der freiwilligen Weitergabe seiner Daten an Dritte das Risiko eingeht, dass die Telefongesellschaft seine Daten der Polizei offenbart. Aus diesem Grund verlangt der vierte Zusatzartikel nicht, dass die Regierung eine gerichtliche Anordnung einholt, bevor sie Anrufmetadaten erhält (Smith v. Maryland, 442 U. S. 735 (747)).

des Inhaltes).[540] So stellte sich heraus, dass eine Kopie jeder elektronischen Kommunikation, die über die Glasfaserkabel übermittelt wurde, die über die *Folsom St.* in das AT&Ts Intranet gelangten, durch die im geheimen Raum installierte Ausrüstung zur NSA geschickt wurde.[541] Um diese Daten zu sammeln, musste die Regierung eine Anordnung des Abschnitts 215 vom FISC erhalten. Sie konnte vor dem FISC beantragen, diese Daten von anderen Unternehmen zu erfragen, solange die Daten für eine terroristische Untersuchung relevant waren. Die nach dem Abschnitt 215 erlangten Daten, die sich auf US-Bürger bezogen, konnten nur an das FBI oder andere Nachrichtendienste weitergegeben werden, und die Hinweise aus den Metadaten beschränkten sich auf Antiterrorismusuntersuchungen.[542] Mit dem Abschnitt 215 war auch die parlamentarische Kontrolle für das FISA-Programm eingerichtet, indem das DOJ (U.S. Department of Justice) dazu aufgefordert wurde, eine Prüfung des Programms und der Wirksamkeit des Abschnitts 215 durchzuführen.

Unter den eigenen Befugnissen (*inherent powers*) des Präsidenten und der Verwaltung verfügte die NSA über die Ermächtigung, US-Amerikaner innerhalb des Landes ohne eine gerichtliche Anordnung zu überwachen, solange sich eine Partei außerhalb der USA befand und der Analytiker vermutete, eine Partei sei ein Terrorist oder ein Mitarbeiter oder Mitglied einer mit dem Terrorismus verbundenen Organisation, insbesondere Al-Qaida.[543] Durch die Enthüllungen des ehemaligen NSA-Mitarbeiters *Snowden* wurde offengelegt, dass die US-amerikanischen Nachrichtendienste im Laufe von sieben Jahren täglich Massentelefonmetadaten für jeden Anruf gesammelt hatten, die Kunden multinationaler Telekommunikationsunternehmen tätigten.[544] Vor Snowdens Enthüllungen entschied der FISC, dass die Massentelefoniemetadatensammlung gemäß dem Abschnitt 215 gerechtfertigt sei. Wegen dieses Umstands hatte das Parlament die neuen

---

540 *Kadidal*, NSA Surveillance: The Implications For Civil Liberties, S. 444.

541 Hepting v. AT&T, No. 06-17131 (9th Cir. 2007).

542 *Reid*, NSA and DEA Intelligence Sharing: Why it is legal and why REUTERS and the GOOD WIFE got it wrong, SMU Law Review, Vol. 68 Issue 2, 2015, S. 437 f.

543 *Reid*, NSA and DEA Intelligence Sharing: Why it is legal and why REUTERS and the GOOD WIFE got it wrong, SMU Law Review, Vol. 68 Issue 2, 2015, S. 440 f.

544 *Greenwald*, NO PLACE TO HIDE: Edward Snowden, the NSA, and the U. S. Surveillance State, 2015.

Rechtsgrundlagen[545] geschaffen, auf denen die NSA auch ohne eine gerichtliche Anordnung zur Überwachung ermächtigt wurde. Abschnitt 702 ermächtigte die Regierung dazu, die Kommunikation außerhalb des traditionellen FISA- oder Titel-III-Anordnungsprozesses zu überwachen, und legte das Verfahren fest, an dem die Überwachung auf die Kommunikation anderer Personen als der US-Bürger, die sich außerhalb der USA befinden, ausgerichtet wird.[546] Im Rahmen des Abschnitts 702 wurden *minimization procedures*[547] geschaffen, damit die *privacy* der versehentlich überwachten US-Bürger geschützt werden kann.

Durch den Foreign Intelligence Surveillance Act von 1978 und den FISA Amendments Act von 2008 wurde ein Verfahren implementiert, das die Massenüberwachung in gewissem Maß begrenzt: gerichtliche Kontrolle, parlamentarische Kontrolle und *minimization procedures*. Die Metadatensammlung der NSA stieß aus verschiedenen Gründen auf Kritik. Zu diesen Gründen gehörte, dass sich das FISC bei seiner Entscheidung auf die von der Regierung vorgelegten Informationen stützte, dass die Mauer zwischen Nachrichtendienst- und Strafverfolgungsbehörden nach den Anschlägen am 11. September 2001 zusammenbrach, dass die Befugnisse der NSA durch den Abschnitt 702 erweitert wurden und dass die Third-Party-Doktrin, deren Zulänglichkeit in der modernen digitalen Gesellschaft zweifelhaft ist, aufrechterhalten wurde.[548] Aber in der *States v. Jones*-Entscheidung stellte das Gericht fest, dass der Massendatensammlung

---

545 Der Protect America Act aus dem Jahr 2007, Pub. L. No, 110–55, 121 Stat. 552 (codified at 50 U. S. C. §§ 1805a to 1805c (2003 & Supp. 2014) als ein Übergangsgesetz und als Rechtsnachfolger des FISA Amendments Act of 2008, H. R. 6304, 110th Cong. (2007–2008) – ist ansonsten als Abschnitt 702 oder FAA bekannt.

546 50 U. S. C. § 1881 (a) (2003 & Supp. 2014).

547 Sie legen die Voraussetzungen fest, unter denen der Inhalt und die Identität der US-Bürger, die versehentlich überwacht wurden, gelöscht werden müssen. Dazu ausführlich *Reid*, NSA and DEA Intelligence Sharing: Why it is legal and why REUTERS and the GOOD WIFE got it wrong, SMU Law Review, Vol. 68 Issue 2, 2015, S. 442 f.

548 Der Kern dieser Doktrin, deren Ursprung in dem Fall Smith v. Maryland zu finden ist, besteht darin, „dass einer Person eine subjektive Erwartung der Privatsphäre in Bezug auf Daten fehlt, die mit einem Dritten geteilt werden." Die Doktrin beseitigt die Möglichkeit eines Verstoßes gegen den vierten Verfassungszusatz, weil keine begründete Erwartung der *privacy* in den Metadaten bestand, da die Kunden ihre Daten mit einem Drittanbieter austauschten. Diesbezüglich erhöhte sich die Forderung nach einer nochmaligen Überlegung der Third-Party-Doktrin (siehe *Barnett*, Why the NSA Data Seizures are unconstitutional, Harvard Journal of Law & Public Policy, Vol. 38 No. 1, 2014, S. 10 ff.).

besondere Bedeutung zukommen kann, obwohl die gesammelten Daten freiwillig an Dritte weitergegeben wurden.[549] Das Gericht entschied, dass eine begründete Erwartung in puncto *privacy* in bestimmten Datenmengen anerkannt wird, selbst wenn solche Erwartungen in ihren Bestandteilen nicht angenommen werden können.[550]

bb) Der Freedom Act nach den Snowden-Enthüllungen

Die Metadatensammlung der NSA hat durch die Verabschiedung des Freedom Act eine neue Phase erreicht. Nach Snowdens Enthüllungen wurden die Recht- und Verfassungsmäßigkeit des Metadatensammlungsprogramms der NSA für Massentelefonie in zwei bedeutsamen Fällen[551] bestritten, die in Erwägungen über eine einstweilige Anordnung zu völlig unterschiedlichen Ergebnissen führten. Das Parlament hat daher im Jahr 2015 ein neues Gesetz[552] erlassen, um dabei zu helfen, Rechtsstreitigkeiten beizulegen und das Metadatensammlungsprogramm der NSA für Massentelefonie unter strengere Voraussetzungen zu stellen. Das Gesetz zielt vor allem auf die Beendigung der Massenverbindungsdatensammlung durch die NSA.

Das Gesetz brachte zwei bedeutende Änderungen mit sich: Die erste Änderung betrifft die Einführung eines neuen, eng eingeschränkten Mechanismus für die gezielte Sammlung von Telefonmetadaten für mögliche Verbindungen zwischen ausländischen Mächten oder Vertretern ausländischer Mächte und anderen Personen vor, die im Rahmen einer be-

549 United States v. Jones, 132 S. Ct. 945 (2012).

550 *Gray/Citron*, A Shattered Looking Glas: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy, North Carolina Journal of Law and Technology, Vol. 14, No. 2, 2013, 381, 381-382.

551 ACLU v. Clapper, 959 F. Supp. 2d 724 (S. D. N. Y. 2013) (Die Beschwerde wurde teilweise mit der Begründung abgelehnt, dass die Kunden im Rahmen des Präzedenzfalles des vierten Verfassungszusatzes keine berechtigten Erwartungen auf *privacy* in telefonischen Metadaten haben, die ein Dritter besitzt) und 785 F. 3d. 787 (2nd Cir. 2015); Klayman v. Obama, 957 F. Supp. 2d 1, 9 (D. D. C. 2013) (Es wurde festgestellt, dass das Gericht zwar für die Überprüfung des Antrags auf den Administrative Procedure Act (APA) nicht zuständig war, aber konstitutionelle Herausforderungen für das Verhalten der NSA behandeln konnte. Hier wurde einem Antrag auf einstweilige Anordnung stattgegeben.)

552 USA FREEDOM Act (the Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act), H. R. 3361, 113th Cong. (2013–2014).

fugten Ermittlung zum Schutz vor internationalem Terrorismus verfolgt werden. Es wird hier vorausgesetzt, dass die Regierung eine FISC-Anordnung für Metadatensätze einholen muss, die direkt von Unternehmen aufbewahrt werden, erst nachdem eine bestimmte Person, ein Konto, eine Adresse oder ein anderer spezifischer Identifikator als Gegenstand einer spezifischen Untersuchung bestimmt wurde.[553] Wird die gerichtliche Anordnung erteilt, muss der Telekommunikationsanbieter oder ein anderer Unternehmensanbieter die Metadatensätze gemäß einer spezifischen Untersuchung erstellen.[554] Die Verbindungsdaten wurden also vorher von der NSA massenhaft gespeichert. Aber diese werden gemäß diesem Gesetz von den Telekommunikationsanbietern gespeichert und nur noch auf Anfrage bereitgestellt. Die zweite Änderung bezieht sich auf die Forderung nach mehr Transparenz und öffentlicher Berichterstattung über die nationalen Sicherheitsprogramme. In diesem Zusammenhang wurden einige Verfahren eingerichtet: zusätzliche Benachrichtigung an das Parlament, jährliche öffentliche Transparenzberichte sowie Benachrichtigungsmöglichkeit im Privatsektor, die vor Einführung des USA Freedom Act (USAF) wegen der geheimen Natur der FISA-Anordnung ausgeschlossen wurde. Aber das USAF gibt Unternehmen die Möglichkeit, ihre Kunden sowohl in den USA als auch im Ausland über das Volumen und die Arten der nationalen Sicherheitsanfragen zu informieren, die sie erhalten. Das USAF verlangt also von den Geheimdiensten mehr Transparenz bezüglich der von ihnen gesammelten Daten. Die Telekommunikationsanbieter unterliegen nicht mehr der Anordnung, die sie daran hindert, ihre Kunden darüber zu informieren, dass ihre privaten Daten an die Regierung übermittelt werden. Durch die Einführung des USAF wurden die folgenden Maßnahmen mög-

553 USA FREEDOM Act of 2015, Pub. L. No. 114-23, § 101 (a) (3), 129 Stat. 268, 26970 (codified at 50 U.S.C. § 1861 (b) (2) (C) (2016)) ("[An] application for the production on a daily basis of call detail records […] conducted to protect against international terrorism. "a statement of facts showing that […] (i) there are reasonable grounds to believe that the call detail records sought to be produced based on the specific selection term required […] are relevant to such investigation; and (ii) there are facts giving rise to a reasonable, articulable suspicion that such specific selection term is associated with a foreign power or an agent of a foreign power.").

554 USA FREEDOM Act of 2015, § 101 (b), 129 Stat. at 270; *Steinhauer/Weisman*, U. S. Surveillance in Place Since 9/11 is Sharply Limited, The New York Times v. 2.6.2015, abrufbar unter: https://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html: "The storage of those records now shifts to the phone companies, and the government must petition a special federal court [FISC] for permission to search them."

lich, die zu mehr Transparenz führen: Freigabe von FISC-Stellungnahmen mit wesentlichen rechtlichen Auslegungen, ein institutionalisierter Prozess für die Teilnahme von *Amicus Curiae* und der Ersatz des weitgehend einseitigen FISC-Prozesses – also einer fehlenden Berufungsmöglichkeit – durch das Berufungsgericht, das *Foreign Intelligence Surveillance Court of Review* (FISCR).

Der Freedom Act ist mit Blick auf die individuelle Freiheit und die Privatsphäre gegenüber dem PATRIOT Act zwar als eine Verbesserung anzusehen, reicht jedoch noch nicht weit genug. Denn das Gesetz schränkt nur die Massenmetadatensammlung der NSA bezüglich des Abschnitts 215 PATRIOT Act, aber nicht die Massenmetadatensammlung selbst ein. Damit ist nicht die Beauftragung der anderen Behörden mit der Massenmetadatensammlung verboten. Außerdem ist die Regulierung der Massenmetadatensammlung bezüglich E-Mails, Internetsuche und Web-Browser-Verläufen ausgeschlossen.[555] Die Datenspeicherung in einer Datenbank durch die Regierung mit einzelnen *subpoenas* wird ebenfalls noch vertreten. Durch die Verpflichtung zur Datenspeicherung beim Telekommunikationsunternehmen würden diesem Kosten auferlegt, Innovationen behindert und der Zugang zu ICT eingeschränkt.[556] Es wird die Meinung vertreten, dass Drittanbieter diese Daten höchstwahrscheinlich nicht über einen längeren Zeitraum aufbewahren werden, und auch wenn sie dazu aufgefordert werden, würden sie eine beträchtliche Gebühr von der Regierung verlangen oder die Kosten an die Verbraucher weitergeben. Die Daten würden dann in die Hände einer dritten Partei gelangen, wobei die Kontrolle der Datenbank durch staatliche Einrichtungen wie dem Kongress nur in einem geringen oder unwesentlichen Maße möglich wäre.[557] Angesichts des Gefährdungspotenzials der Privatsphäre des Einzelnen durch die Regierung und der außergewöhnlicher Aussagekraft der Metadaten ist diese Ansicht nicht vertretbar.

555 *Hu*, Bulk Biometric Metadata Collection, North Carolina Law Review, Vol. 96, 2018, S. 1469.

556 *Center for Democracy and Technology*, Introduction to Data Retention Mandates, 2012, S. 5.

557 *Reid*, NSA and DEA Intelligence Sharing: Why it is legal and why REUTERS and the GOOD WIFE got it wrong, SMU Law Review, Vol. 68 Issue 2, 2015, S. 454.

2. Aktuelle Rechtslage

Um das Freiheits- und Persönlichkeitsinteresse des Einzelnen zu schützen, garantiert der vierte Verfassungszusatz das Recht, frei von einer unbegründeten Durchsuchung und Beschlagnahme zu sein. Eine begründete Durchsuchung und Beschlagnahme setzt eine gerichtliche Anordnung voraus, die auf der Wahrscheinlichkeit einer Straftat basiert (*warrant on probable cause*). Diese Anordnung ist nach der Katz-Entscheidung beim Vorliegen der begründeten Erwartung auf *privacy* notwendig. Die Telekommunikationsdaten werden auch im Kontext des vierten Verfassungszusatzes geschützt. Danach dürfen sie nur mit einem gerichtlichen Befehl durchsucht und in Beschlag genommen werden. Dies beruht auf der Entscheidung *Katz v. United States* von 1967, nach der der vierte Verfassungszusatz nicht nur die Beschlagnahme von materiellen Gegenständen regelt, sondern sich auch auf die Aufzeichnung mündlicher Aussagen erstreckt.[558] Nachdem sich herausgestellt hatte, dass die Telekommunikationsdaten der Bürger ohne diese fundamentale Voraussetzung einer gerichtlichen Anordnung durch die Nachrichtendienste erhoben und gespeichert wurden, standen die USA unter Schock. Die Snowden-Enthüllungen führten zu Einschränkungen in diesem Bereich.

Den Betroffenen ist die Überwachung in der Regel nicht bewusst. Die Aussagekraft dieser Daten ist weitreichend, weil sich bei umfassender und automatisierter Auswertung aus diesen Daten inhaltliche Rückschlüsse ziehen lassen, die bis in die Intimsphäre hineinreichen. Bei der weiteren Nutzung der Telekommunikationsdaten und bei zunehmender Dichte könnten eine Speicherung und eine Nutzung der Telekommunikationen die Erstellung aussagekräftiger Persönlichkeits- und Bewegungsprofile praktisch jedes Bürgers ermöglichen. Die Telekommunikationsüberwachung greift in dieser Hinsicht intensiver in Grundrechte ein als normale Durchsuchungen. Dies gilt nicht nur im Bereich des Nachrichtendienstes, sondern auch im Bereich der Strafverfolgung. In Anbetracht dieser Gefahr der Telekommunikationsüberwachung hat das US-Parlament zum Ziel des Privatsphärenschutzes der Bürger im Jahr 1968 den Federal Wiretap Act von 1968 (*Title III of Omnibus Crime Control and Safe Streets Act*)[559] erlassen, dem gemäß die absichtliche Überwachung kabelgebundener Kommunikationen verboten ist, außer wenn eine gesetzliche Ausnahme angewandt wird. Da der Act nur die kabelgebundene Kommunikation zum Gegen-

558 Katz v. United States, 389 U. S. 347 (347).
559 Pub. L. 90-351, June 19, 1968, 82 Stat. 42 U. S. C. § 3711.

stand hatte, bedurfte es einer Gesetzesanwendung auch auf die drahtlosen Kommunikation. Der Electronic Communications Privacy Act (ECPA) von 1986[560] hat damit den Title III (den Federal Wiretap Act) geändert und zwei weitere Gesetze als Reaktion auf Entwicklungen in der Computertechnologie und in den Kommunikationsnetzwerken eingeführt: 1. den Wiretap Act (18 U. S. C. §§ 2510–2522); 2. den Stored Communications Act (SCA) (18 U. S. C. §§ 2701–2711); und 3. den Pen Register Act (18 U. S. C. §§ 3121–3127). Danach wurde der USA PATRIOT Act[561] verabschiedet, mit dem geringfügige Änderungen am bestehenden Datenerhaltungsmodell vorgenommen wurden. Mit dem PATRIOT Act wurden Teile des ECPA geändert, wodurch der Zugang der Strafverfolgungsbehörden zu elektronischen Daten verbessert und der Datenschutz der Verbraucher verringert wurde. Der PATRIOT Act erlaubt es Internet Service Providern, Verkehrs- und Standortdaten unter bestimmten Umständen freiwillig an die Strafverfolgungsbehörden weiterzugeben. Das Gesetz erweitert auch die Daten, die die Strafverfolgungsbehörden von einem Diensteanbieter nur mit einer *subpoena* anfordern können – und zwar ohne Benachrichtigung des Betroffenen.[562]

Es wurde bereits erwähnt, dass das US-Gesetzbuch keine Bestimmung zur Vorratsdatenspeicherung enthält, das der in Deutschland gültigen entspricht und die die Anbieter öffentlich zugänglicher elektronischer Kommunikationsdienste oder Betreiber dazu verpflichtet, bestimmte Daten in einem bestimmten Zeitraum auf Vorrat zu speichern.[563] Aufgrund der Erfahrungen der Bürger mit der Datenspeicherungspraxis der Regierung wurde die Einführung der Vorratsdatenspeicherung in den USA trotz mehrerer Gesetzgebungsversuche verhindert. Denn die Regierung hat das Vertrauen der Bürger in ihre Führungspraxis von Telekommunikationsdaten verloren. Während die EU-Staaten auf die Terroranschläge

560 Pub. L. 99-508, October 21, 1986, 100 Stat. 1848. Der Electronic Communications Privacy Act und der Stored Wire Electronic Communications Act werden allgemein als der ECPA von 1986 bezeichnet.

561 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

562 *Ringland*, The European Union's Data Retention Directive and the United States's Data Preservation Laws: Finding the Better Model, 5 Shidler J. L. Com. & Tech. 13, 2009; *Young*, Surfing While Muslim: Privacy, Freedom of Expression & the Unintended Consequences of Cybercrime Legislation, International Journal of Communications Law & Policy, No. 9, 2004.

563 *Crump*, Data Retention: Privacy, Anonymity, and Accountability Online, Stanford Law Review, Vol. 56, 2003, 191.

mit der Vorratsdatenspeicherung reagiert haben, wird in den USA das sog. *Quick-Freeze-Verfahren* oder *Data-Freeze-Verfahren* (das anlassbezogene *Data-Preservation-Modell*) praktiziert,[564] das auch in Europa zuweilen als Alternative zur Vorratsdatenspeicherung vorgeschlagen[565] oder als ein zusätzliches Ermittlungsmittel praktiziert wird. Darunter versteht man ein Verfahren, in dem die Daten einer verdächtigen Person ab dem Zeitpunkt einer polizeilichen Anordnung gegen ein Telekommunikationsunternehmen (oder einen Internet Service Provider) gespeichert und damit „eingefroren" werden.[566] Nach dem US-Internet-Service-Provider-Verein sei das Data-Preservation-Modell „der bevorzugte Mechanismus, um die Gefahr des Löschens von Datensätzen und Kommunikationen zu minimieren, die während einer Ermittlung eines Verbrechens notwendig sein können"[567]. Bei diesem Verfahren geht es um eine allgemeine Kommunikationsdatenanfrage, mit der auf die zu und ab dem Zeitpunkt einer Anordnung noch vorhandenen und entstehenden Telekommunikationsverbindungen zugegriffen wird. Insoweit erfasst ein solches Verfahren allerdings gerade solche Daten nicht, auf die die Vorratsspeicherung abzielt, nämlich diejenigen, die zu Betriebszwecken eines Unternehmens nicht gespeichert werden, und diejenigen, die vor der in der Vorratsdatenspeicherungsregelung vorgesehenen Frist von Telekommunikationsunternehmen gelöscht werden.[568] Außerdem werden Bestands- und Verkehrsdaten in den USA

564 *Ringland*, The European Union's Data Retention Directive and the United States's Data Preservation Laws: Finding the Better Model, 5 Shidler J. L. Com. & Tech. 13, 2009.

565 *Der Deutsche Bundestag*, Plenarprotokoll 16/19, Stenographischer Bericht, 19. Sitzung in der 16. Wahlperiode, Berlin, 16. Feburar2006, S. 1419, abrufbar unter: http://dip.bundestag.de/btp/16/16019.pdf; *Dix*, Freiheit braucht Sicherheit – Sicherheit braucht Freiheit, Benjamin Franklin und die Freiheit zur unbeobachteten Kommunikation, in: *Bundeskriminalamt* (Hrsg.), Informations- und Kommunikationskriminalität, Vorträge anlässlich der Herbsttagung des Bundeskriminalamtes vom 2. bis 4. Dezember 2003, Kriminalistik 2004, S. 82.

566 *Albrecht, H.-J.*, Schutzlücken durch Wegfall der Vorratsdatenspeicherung – Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten: Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht, im Auftrag des Bundesministeriums der Justiz, S. 182.

567 *Petersen*, Toward a U. S. Data-Retention Standard for ISPs, EDUCAUSE Review, Vol. 41, No. 6, 2006, 78-79: "The preferred mechanism to minimize the risk of deletion of records and communications that may be necessary during an investigation of a crime."

568 *Albrecht, H.-J.*, Schutzlücken durch Wegfall der Vorratsdatenspeicherung – Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei

nicht voneinander unterschieden. Während die Datenspeicherung im Rahmen des Nachrichtendienstes bei den staatlichen Stellen selbst geschieht, werden die Kommunikationsdaten nach dem ECPA von Telekommunikationsanbietern gespeichert.

Im Hinblick auf das Quick-Freeze-Verfahren kommt dem Communications Assistance for Law Enforcement Act von 1994 (CALEA)[569] eine wichtige Bedeutung zu. Das Quick-Freeze-Verfahren gewinnt tatsächliche Vollzugskraft durch das CALEA, das die Zusammenarbeit von Dienstleistungsanbietern erzwingt. Das Gesetz schreibt vor, dass Telekommunikationsunternehmen ihre Netze so auslegen müssen, dass sie auf das befugte behördliche Überwachungsersuchen antworten können. Alle Telekommunikationsunternehmen müssen demnach dazu in der Lage sein, elektronische Kommunikationen zu isolieren und zu überwachen und die Daten an die Strafverfolgungsbehörden zu übermitteln. Der Zweck des Gesetzes ist es, die Fähigkeit der Strafverfolgungsbehörden zu verbessern, elektronische Überwachung durchzuführen. Dies geschieht durch die Forderung, dass die Telekommunikationsunternehmen ihre Ausrüstung, Einrichtungen und Dienstleistungen so verändern und gestalten müssen, dass sichergestellt ist, dass diese eingebaute Überwachungsmöglichkeiten haben, sodass Bundesbehörden jede Telekommunikation abhören können.[570] Das CALEA ist also das Gesetz, das die im ECPA geregelte Telekommunikationsüberwachung und das Erlangen von Kommunikationsdaten durch staatliche Behörden ermöglicht. Darin wird die Pflicht eines Telekommunikationsanbieters[571] vorgeschrieben, das Abhören durchzusetzen und der Strafverfolgungsbehörde dessen Ergebnisse zu übermitteln, wenn eine Strafverfolgungsbehörde mit einer gerichtlichen Anordnung oder einer anderen gesetzmäßigen Erlaubnis ein Abhören beantragt. Dabei werden die

---

Fehlen gespeicherter Telekommunikationsverkehrsdaten: Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht, im Auftrag des Bundesministeriums der Justiz, S. 182 f.

569 Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 U. S. C. §§ 1001 – 1010.

570 47 U. S. C. § 1002 (a) (4) (A).

571 Das CALEA gilt nicht für Informationsdienste, ein bedeutsamer und über viele Jahre angewandter Begriff im Telekommunikationsrecht. Es gilt für Telekommunikationsunternehmen. Informationsdienstanbieter fallen nicht unter das CALEA, was bedeutet, dass sie ihre Netzwerke nicht so gestalten müssen, dass sie für Strafverfolgungsbehörden zugänglich sind (vgl. *Solove/Schwartz*, PRIVACY LAW: FUNDAMENTALS, 2011, S. 42); American Council on Education v. FCC, 451 F.3d 266 (D. C. Cir. 2006): Das Gericht bestätigte die FCC-Klassifizierung des Breitband-Internetzugangs und des Voice-over-Internet-Protokolls (VoIP) als Telekommunikationsanbieter gemäß dem CALEA.

Bestands- und Verbindungsdaten in dem Umfang bereitgestellt, in dem der Diensteanbieter sie vernünftigerweise erwerben kann.[572] Nach § 1002 CALEA stellt ein Telekommunikationsanbieter sicher, dass er die zur Überwachung erforderlichen Geräte, Einrichtungen oder Dienstleistungen bereitstellt und bei berechtigtem Verlangen einer staatlichen Behörde eine Überwachung unternimmt sowie ihr Ergebnis an die Stelle übermittelt. Außerdem ist er dazu verpflichtet, bei berechtigtem Verlangen einer staatlichen Behörde die Kommunikationsdaten zu übermitteln, die ihm vernünftigerweise zur Verfügung stehen.

In diesem Zusammenhang geht es im Wiretap Act (18 U. S. C. §§ 2510–2522) um die Überwachung laufender Kommunikationen, also um die Regelungen über das Abhören stimmlicher, digitaler und elektronischer Telekommunikationen, an das nach der Berger-Entscheidung höhere Anforderungen als an die übliche Anordnung gestellt werden. Im SCA (18 U. S. C. §§ 2701–2712) handelt es sich um die Erhebung gespeicherter Kommunikationsdaten nach bereits beendeter Kommunikation, also um den Zugang zu Daten im elektronischen Speicher oder um Daten von ISPs und im Pen Register Act (18 U. S. C. §§ 3121–3127) um die Zulassungsbedingungen eines Gerätes (*Pen Register Device* und *Trap and Trace Device*), das dazu dient, künftige Kommunikationsdaten fortdauernd auszuspähen.[573] Diese verschiedenen Maßnahmen sind mit unterschiedlichen Voraussetzungen verbunden. Unter ihnen ist jedoch ausschließlich der Erhalt von Bestands- und Verbindungsdaten schon beendeter Kommunikationen mit der deutschen Vorratsdatenspeicherung vergleichbar. Da die vorliegende Arbeit auf die Untersuchung der Datenverwendung zum Ziel der Straftatenermittlung in den USA im Vergleich zur deutschen Vorratsdatenspeicherung abzielt, aber nicht auf die Überwachung laufender Kommunikationen, konzentriert sich diese Arbeit hier vornehmlich auf die Behandlung bereits gespeicherter oder künftig zu speichernder Kommunikationsdaten im Sinne des SCA und des Pen Register Act. Die Erhebung künftiger Kommunikationsdaten mit Hilfe eines Gerätes nach dem Pen Register Act unterscheidet sich zwar von der deutschen Vorratsdatenspeicherung dahingehend, dass die staatliche Behörde zukünftige Kommunikationsdaten ab dem Zeitpunkt des Gerätanschlusses erhält. Der Vergleich dieser Maßnahme mit der Vorratsdatenspeicherung ist jedoch insofern

572 47 U. S. C. § 1002.

573 Für eine anschauliche Darstellung der unter dem ECPA zu erhaltenden Daten siehe unten Tabelle 3.

sinnvoll, als die Kommunikationsdaten für einen bestimmten Zeitraum nach dem Anschluss des Geräts gespeichert werden.

Im Folgenden soll untersucht werden, wie, wann und unter welchen Voraussetzungen welche Daten zum Ziel der Straftatenermittlung unter dem US-amerikanischen Ansatz nach dem ECPA gespeichert und verwendet werden dürfen.

Tabelle 3: Die Klassifikation der unter dem ECPA zu erhaltenden Daten

ECPA	Wiretap Act	Kommunikations-überwachung	
	SCA	Die Erhebung gespeicherter Kommunikationsdaten nach der Beendigung der Kommunikation	Kommunikations-inhalte im elektronischen Speicher
			Kommunikations-inhalte im *Remote Computing Service*
			Bestands- und Verbindungsdaten bezüglich des elektronischen Kommunikations-dienstes oder des *Remote Computing Service*
	Pen Register Act	Der Erhalt von Bestands- und Verbindungsdaten bezüglich künftiger Kommunikationen	

a) Zu speichernde Daten

Anstatt die zu speichernden Telekommunikationsdaten konkret und eingeschränkt zu regeln, bleibt die Speicherpraxis von Bestands- und Verkehrsdaten der Entscheidung der Telekommunikationsanbieter überlas-

sen.[574] Denn es existieren in den USA für den Privatsektor so gut wie keine Datenschutzregelungen. Während bei der ehemaligen Speicherpraxis der Daten durch die NSA die staatliche Behörde die Daten, die von den Telekommunikationsanbietern täglich übertragen werden, von sich aus speichert, werden die Daten hier von den Telekommunikationsanbietern auf Antrag der staatlichen Behörde für einen bestimmten Zeitraum gespeichert. Anstatt zu speichernde Telekommunikationsdaten zu regulieren, bestimmt das ECPA Datenarten, die Telekommunikationsanbieter auf Antrag einer staatlichen Stelle an sie übermitteln sollen. 18 U. S. C. § 2703 (c) sieht vor, dass ein Anbieter eines elektronischen Kommunikationsdienstes oder eines *remote computing service* einen Datensatz oder andere Informationen über seine Kunden (außer den Kommunikationsinhalten) auf Antrag einer befugten Behörde offenlegen soll – Namen, Adressen, Listen von Fernsprechanschlüssen, Daten über die Anzahl und die Dauer der Anrufe in einem bestimmten Zeitraum, die Dienstdauer (einschließlich des Anfangsdatums) und die Art der benutzten Dienste und Zahlungsmittel (einschließlich Kreditkarten- oder Bankkontonummer). Hierbei hängen die Daten, die die staatlichen Behörden erhalten, von der Datenspeicherungspraxis des betreffenden Unternehmens ab. Dies liegt daran, dass nur die Daten, die das Unternehmen bereits vor dem Antrag der Behörde aufbewahrt hat, durch die Maßnahme abgerufen werden können. Da die USA jedoch kaum oder gar nicht über Regelungen zum Datenschutz im privaten Sektor verfügen, wird die Vorschrift letztendlich die Arten von Daten einschränken, die die Behörde erhalten darf. Anstatt die Art der Daten festzulegen, die vorab gespeichert werden müssen, ist das Unternehmen nach dem CALEA nur dazu verpflichtet, die Kommunikationsdaten an die berechtigte Stelle zu übermitteln, die ihm vernünftigerweise zur Verfügung stehen, damit der Verlust erforderlicher Daten bei der Datenanfrage verhindert wird.

Darüber hinaus können auch die zukünftigen Verbindungsdaten mit einem *Pen Register Device* oder einem *Trap and Trace Device* erhoben werden. Das *Pen Register Device* registriert oder dekodiert die Wähl-, Routing-, Adressierungs- und Signalisierungsinformationen, die durch ein Instrument oder eine Einrichtung übertragen werden, von der die kabelgebundenen oder elektronischen Kommunikationen übertragen werden (§ 3127 (3) ECPA). Das *Trap and Trace Device* erfasst eingehende elektronische oder andere Impulse, die die Ursprungsnummer oder andere Wähl-, Rou-

574 *Büllingen*, Vorratsspeicherung von Telekommunikationsdaten im internationalen Vergleich, DuD 2005, 349, 351 f.

ting-, Adressierungs- und Signalisierungsinformationen identifizieren, die die Quelle einer kabelgebundenen oder elektronischen Kommunikation mit angemessener Wahrscheinlichkeit identifizieren. Ein *Trap and Trace Device* zeigt also, welche Rufnummern ein bestimmtes Telefon gewählt hat, d. h. alle eingehenden Telefonnummern, während ein Pen-Register eher zeigt, welche Rufnummern ein Telefon angerufen hat, also alle Telefonnummern von ausgehenden Anrufen. Die durch diese Geräte gewonnenen Daten gehören zu den Verkehrsdaten, die eine staatliche Behörde zur Strafverfolgung verwenden kann.

b) Zugriff auf Daten

Auf die Daten, die die Telekommunikationsanbieter auf Antrag einer staatlichen Behörde gespeichert haben, darf je nach Datenarten unterschiedlich zugegriffen werden. Das ECPA schließt also den Zugriff entsprechend den Typen von staatlichen Behörden angefragter Daten an unterschiedliche Anforderungen an. Der Unterschied bezüglich der Anforderungen beruht auf dem verschiedenen Schutzniveau der *privacy*. Das ECPA stellt damit für die Überwachung laufender Kommunikationen die höchsten Anforderungen, für den Zugriff auf schon gespeicherte Kommunikationsinhalte die üblichen Anforderungen, für den Zugriff auf vergangene Bestands- und Verkehrsdaten die erleichterten Anforderungen und für den Zugriff auf künftige Bestands- und Verkehrsdaten durch die Installation des *Pen Register* oder der *Trap and Trace Devices* die am meisten erleichterte Anforderung. Die Voraussetzungen unter dem ECPA finden aber dann keine Anwendung, wenn die Betroffenen zustimmen. Um zu erklären, wie auf die Daten zugegriffen werden kann, die mit den durch die deutsche Vorratsdatenspeicherung erhobenen Daten vergleichbar sind, sollen hier ausschließlich die Zugriffsvoraussetzungen der beim ISP schon in Bewahrung stehenden vergangenen Verkehrsdaten erörtert werden.

Um die vergangenen Verkehrsdaten zu erheben, muss eine staatliche Behörde zuerst den Telekommunikationsdienstanbietern die Speicherung dieser Daten gebieten. Der Anbieter ergreift auf Ersuchen dieser Stelle alle erforderlichen Maßnahmen, um die Daten und die anderen in seinem Besitz befindlichen Beweismittel bis zur Erteilung einer gerichtlichen Anordnung oder zu anderen Verfahren aufzubewahren. Die Daten sind neunzig Tage lang aufzubewahren, wobei diese Frist auf erneuten Antrag der staatlichen Stelle um weitere neunzig Tage verlängert werden kann. Die auf diese Weise gespeicherten Daten dürfen durch diese Stelle nur

unter bestimmten Voraussetzungen erhoben werden. Eine staatliche Behörde kann von einem Telekommunikationsdienstanbieter die Übermittlung dieser Daten (außer dem Kommunikationsinhalt) nur dann verlangen, wenn die Behörde von einem zuständigen Gericht einen *warrant* erwirbt, wenn die Behörde eine gerichtliche Anordnung für eine solche Offenlegung erhält, indem sie spezifische und klare Tatsachen darstellt, aus denen ersichtlich ist, dass Grund zu der Annahme besteht, dass die angeforderten Daten für eine laufende strafrechtliche Untersuchung relevant und wesentlich sind, wenn die Behörde die Zustimmung des Betroffenen zu einer solchen Offenlegung erhält, wenn die Behörde einen formellen schriftlichen Antrag einreicht, der von einer Strafverfolgungsuntersuchung in Bezug auf Telemarketing-Betrug betroffen ist oder wenn die Behörde die bestimmten Daten mit einer *subpoena* sucht: den Namen, die Adresse, die Telefonverbindungsdaten oder die Daten über Verbindungszeiten und -dauer, die Dienstdauer (einschließlich Startdatum) und die Art der in Anspruch genommenen Dienste, die Telefon- oder Instrumentennummer oder die Nummer oder die Identität anderer Teilnehmer (einschließlich einer vorübergehend zugewiesenen Netzwerkadresse) und die Zahlungsmittel und -quelle für diese Dienstleistung (einschließlich Kreditkarten- oder Bankkontonummer).

Dementsprechend können vergangene Verkehrsdaten im Fall der Nutzung mobiler Telefondienste unter der erleichterten Voraussetzung gemäß 18 U. S. C. § 2703 (c) erhoben werden. Dabei kann sich aus den Bezeichnungen der Funkzellen, die durch den anrufenden und den angerufenen Anschluss während der Verbindung genutzt wurden, die überschlägige geografische Lage des genutzten mobilen Telefons ergeben. Unter Berücksichtigung der Größe der Personen werden deren Standortdaten an öffentlichen Orten grundsätzlich nicht durch die begründete Erwartung auf *privacy* geschützt, solange sie sich nicht absichtlich mit bedecktem Gesicht bewegen. Im Karo-Fall entschied der Supreme Court, dass ein *warrant* erforderlich ist, damit ein GPS-Tracker an eine Person oder an ihre Besitztümer angeschlossen werden kann, da dadurch der Standort im Innenraum bekannt gemacht wird, der mit bloßem Auge nicht sichtbar ist.[575] Aus der gleichen Logik ergibt sich, dass für die Anschließung des GPS-Trackers an

575 United States v. Karo, 468 U. S. 705 (1984). In diesem Zusammenhang entschied der Supreme Court, dass für die Positionierung in Innenräumen durch eine Wärmebildkamera ein *warrant* eingeholt werden muss (Kyllo v. United States, 533 U. S. 27).

ein Auto kein *warrant* erforderlich ist.[576] Diese Entscheidungen wurden ursprünglich so interpretiert, dass nur für die Positionierung in Innenräumen ein *warrant* erforderlich ist. Praktisch wird jedoch anerkannt, dass die Nutzung aller Positionstracker warrant-pflichtig ist, sodass die Bundespolizei zur Installation eines Positionstrackers regelmäßig einen *warrant* beantragt.[577] Hierbei kann die Frage gestellt werden, ob die Standortdaten eines mobilen Telefons durch die Bezeichnungen der Funkzellen mit einem Standorttracker vergleichbar sind, der an eine Person oder an ihre Besitztümer so angeschlossen wird, dass der Standort im Innenraum bekannt gemacht wird, der mit bloßem Auge nicht sichtbar ist. Wenn die Frage bejaht wird, muss die weitere Frage gestellt werden, ob die Erhebung der vergangenen Verkehrsdaten im Fall der Nutzung mobiler Telefondienste unter der erleichterten Voraussetzung gemäß dem ECPA in einem angemessenen Verhältnis zur Eingriffsintensität steht. Diesen Fragen kommt eine Bedeutung zu, weil die Voraussetzungen davon abhängen, wie das Wesen der Standortdaten des mobilen Telefons durch die Bezeichnungen der Funkzellen zu begreifen ist. Wenn die Standortdaten des mobilen Telefons durch die Bezeichnungen der Funkzellen zu den vergangenen oder zukünftigen Verkehrsdaten gehören, wäre es möglich, sie unter den erleichterten Voraussetzungen – gemäß dem SCA oder den am meisten erleichterten Voraussetzungen gemäß dem Pen Register Act – zu erheben, während sie, wenn sie als ein Standorttracker anzusehen sind, unter den normalen Voraussetzungen erhoben werden müssten. Da das ECPA über keine Einschränkung auf die Bezeichnungen der Funkzellen, die durch den anrufenden und den angerufenen Anschluss *bei Beginn der Verbindung* genutzt wurden, verfügt und sich die Telekommunikationstechnik immer noch entwickelt, kann man nicht gänzlich die Möglichkeit ausschließen, dass die Standortdaten des mobilen Telefons durch die Bezeichnungen der Funkzellen mit einem Standorttracker vergleichbar sind. Einige Gerichte entschieden, dass die Bezeichnungen der Funkzellen während der Verbindung sowie bei Beginn oder Ende der Verbindung unter den Vorausset-

576 U. S. v. Moran, 349 F. Supp.2d 425 (N. D. N. Y. Jan 05, 2005).

577 U. S. v. In re Application for Tracking Devices on a White Ford Truck, 155 F. R. D. 401, 403 (D. Mass. 1994).

zungen des SCA oder des Pen Register Act erhoben werden dürfen.[578] Andere Gerichte kamen jedoch zu einem umgekehrten Ergebnis.[579]

Der Pen Register Act sieht vor, dass die Installation oder die Verwendung des *Pen Register* oder eines *Trap and Trace Device* grundsätzlich einer richterlichen Anordnung auf Antrag der Staatsanwaltschaft bedarf (18 U. S. C. §§ 3122 und 3123).[580] Für diese Anordnung genügt eine Bescheinigung, die besagt, dass die Daten, die möglicherweise durch eine Installation oder Verwendung eines solchen Geräts erhalten werden, für eine laufende strafrechtliche Untersuchung relevant sind (§ 3122 (b) (2)). Bei einem dringenden Fall kann die gerichtliche Anordnung nachträglich – innerhalb von 48 Stunden nach der Installation des Geräts – eingeholt werden.[581] Dabei soll die Maßnahme dann beendet werden, wenn die gesuchten Informationen gewonnen wurden, wenn der Antrag auf eine

578 In re Application of U. S. for an Order for Prospective Cell Site Location Information on a Certain Cellular Telephone, S. D. N. Y. 2006, 460 F. Supp. 2d 448.

579 In re U. S. for an Order Authorizing the Release of Prospective Cell Site Information, D. D. C. 2006, 407 F. Supp. 2d 134.

580 In der *Smith v. Maryland*-Entscheidung stellte das Gericht unter Anwendung der third party doctrine fest, dass Strafverfolgungsbehörden keine gerichtliche Anordnung aufgrund eines *probable cause* im Kontext des vierten Verfassungszusatzes benötigen, um ein sogenanntes „Pen-Register" auf einem Telefonkonto zu installieren, das die angerufenen Nummern und die Dauer der Anrufe aufzeichnet und meldet, nicht jedoch den Inhalt der Gespräche (442 U. S. 735, 741 ff.).

581 § 3125 – Emergency pen register and trap and trace device installation
(a) Notwithstanding any other provision of this chapter, any investigative or law enforcement officer, specially designated by the Attorney General, the Deputy Attorney General, the Associate Attorney General, any Assistant Attorney General, any acting Assistant Attorney General, or any Deputy Assistant Attorney General, or by the principal prosecuting attorney of any State or subdivision thereof acting pursuant to a statute of that State, who reasonably determines that—
(1) an emergency situation exists that involves—
(A) *immediate danger of death or serious bodily injury to any person*;
(B) *conspiratorial activities characteristic of organized crime*;
(C) *an immediate threat to a national security interest*; or
(D) *an ongoing attack on a protected computer (as defined in section 1030) that constitutes a crime punishable by a term of imprisonment greater than one year*;
that requires the installation and use of a pen register or a trap and trace device before an order authorizing such installation and use can, with due diligence, be obtained, and
(2) there are grounds upon which an order could be entered under this chapter to authorize such installation and use;

gerichtliche Anordnung abgewiesen wurde oder wenn seit dem Beginn der Maßnahmen 48 Stunden abgelaufen sind. Zum Einsatz dieser Maßnahme sind also weder eine Anlasstat noch ein Straftatbezug erforderlich. Nur mit Relevanz für eine laufende strafrechtliche Untersuchung – auch mit Wesentlichkeit bei schon gespeicherten Kommunikationsdaten außer Inhalten – dürfen also die schon gespeicherten oder die künftigen Kommunikationsdaten außer Inhalten angefordert und übermittelt werden. Die staatlichen Behörden weisen den jeweiligen Telekommunikationsanbieter an, noch vorhandene und anfallende Daten „einzufrieren" und zu speichern. Auf Ersuchen einer Behörde ergreift der Telekommunikationsanbieter alle erforderlichen Maßnahmen, um die in seinem Besitz befindlichen Daten und sonstige Beweismittel aufzubewahren, bis eine gerichtliche Anordnung erteilt wird oder ein anderes Verfahren vorliegt. Die Behörde kann dann mit einer gesetzmäßigen Befugnis (einer gerichtlichen Anordnung, der Zustimmung oder einer *subpoena*) auf die Daten zugreifen.

Zusammenfassend schließt sich die – sowohl durch das sog. Quick-Freeze-Verfahren als auch durch den Einsatz eines Gerätes geschehene – Erhebung von Kommunikationsdaten außer Inhalten, die mit der deutschen Vorratsdatenspeicherung vergleichbar sind, weder an den Verbrechenskatalog als eine Anlasstat noch an die Zweckbindung an. Da das ECPA die speziellen Zwecke, für die die Daten erhoben werden dürfen, nicht erwähnt, ist die Verwendung der erhobenen Daten und damit auch ihre Weitergabe nicht eingeschränkt. Obwohl kein bestimmter Verdacht auf eine Anlasstat erforderlich ist, darf auf die Daten nur mit einer erleichter-

---

may have installed and use a pen register or trap and trace device if, *within forty-eight hours after the installation has occurred, or begins to occur, an order approving the installation or use is issued in accordance with section 3123 of this title*.
(b) In the absence of an authorizing order, such use shall immediately terminate when the information sought is obtained, when the application for the order is denied or when forty-eight hours have lapsed since the installation of the pen register or trap and trace device, whichever is earlier.
(c) The knowing installation or use by any investigative or law enforcement officer of a pen register or trap and trace device pursuant to subsection (a) without application for the authorizing order within forty-eight hours of the installation shall constitute a violation of this chapter.
(d) A provider of a wire or electronic service, landlord, custodian, or other person who furnished facilities or technical assistance pursuant to this section shall be reasonably compensated for such reasonable expenses incurred in providing such facilities and assistance.

ten Anordnung zugegriffen werden.[582] Angesichts der Aussagekraft dieser Kommunikationsdaten bleibt die Zugriffsvoraussetzung auf einem erheblich niedrigen Niveau: 1. der Darstellung spezifischer und klarer Tatsachen, aus denen ersichtlich ist, dass ein Grund zu der Annahme besteht, dass der Kommunikationsinhalt oder die angeforderten Telekommunikationsdaten für eine laufende strafrechtliche Untersuchung relevant und wesentlich sind; 2. einer Bescheinigung, die besagt, dass die Daten, die möglicherweise durch eine Installation oder Verwendung eines solchen Geräts erhalten werden, für eine laufende strafrechtliche Untersuchung relevant sind; oder 3. sogar einer exekutiven *subpoena*. Die einzelnen Übermittlungsverfahren der Daten zur Datensicherheit wie etwa Verschlüsselung sind nicht geregelt. Es ist nur geregelt, dass Telekommunikationsunternehmen alle erforderlichen Schritte unternehmen müssen, um Aufzeichnungen und andere Beweise in ihrem Besitz bis zur Erteilung einer gerichtlichen Anordnung oder zu anderen Verfahren zu erhalten, wenn sie von staatlichen Behörden angefragt werden. Nach dem CALEA ist ein Telekommunikationsbetreiber also nur dazu verpflichtet, einer staatlichen Behörde durch technische und organisatorische Maßnahmen zu ermöglichen, eine Kommunikation zu überwachen oder die Kommunikationsdaten zu erheben und zu verwenden. Er ist aber gesetzlich nicht dazu verpflichtet, seine Datenübermittlung an eine staatliche Behörde gegen unbefugte Kenntnisnahme und Verwendung zu schützen. Zur Transparenz der Datenverwendung berichtet der Generalstaatsanwalt dem Kongress jährlich über die Anzahl der Anordnungen des *Pen Register* und des *Trap and Trace Device*, die von Strafverfolgungsbehörden des Justizministeriums beantragt werden. Der Bericht enthält die Daten über die Dauer des durch eine gerichtliche Anordnung ermächtigten Abhörens sowie die Anzahl und Dauer einer etwaigen Verlängerung der Anordnung, die in der Anordnung angegebene Straftat, die Anzahl der betroffenen Untersuchungen, die Anzahl und das Wesen der betroffenen Anlagen und die Identität des Antragstellers oder der Strafverfolgungsbehörde, die die Anordnung stellt, und die Person, die die Anordnung erteilt.[583]

582 Für die unterschiedlichen Voraussetzungen je nach Typen der angefragten Daten siehe Tabelle 4.

583 18 U. S. C. § 3126.

Tabelle 4: Voraussetzungen nach Typen der angefragten Daten

Datenarten		Voraussetzungen	
Überwachung laufender Kommunikationen		Super warrant	*Warrant* (*probable cause*) Subsidiarität (Die Überwachung ist auf andere Weise gescheitert, wahrscheinlich erfolglos oder zu gefährlich.) Minimization process und bestimmte Verbrechen (predict offenses)
Für 180 Tage oder kürzer gespeicherte Kommunikationen		Üblicher Warrant	*Warrant* (*probable cause*)
Länger als 180 Tage gespeicherte Kommunikationen	Ohne Vorankündigung	Üblicher Warrant	*Warrant* (*probable cause*)
	Mit Vorankündigung	Erleichterte Voraussetzungen	*subpoena* oder gerichtliche Anordnung (Proof of specific and articulable facts showing relevance)
Bestands- und Verkehrsdaten vergangener Kommunikationen (ISP-Records)		Erleichterte Voraussetzungen	*Warrant* (*probable cause*); gerichtliche Anordnung; (proof of specific and articulable facts showing relevance);

		Zustimmung des Betroffenen; förmlicher schriftlicher Antrag oder *subpoena*
Bestands- und Verbindungsdaten bezüglich künftiger Kommunikationen	Am meisten erleichterte Voraussetzungen	gerichtliche Anordnung (certification of relevance)

Das Datenanfrageverfahren ist bei den Geheimdiensten im Rahmen der Terrorabwehr ein anderes.[584] Das FBI darf einen Telekommunikationsanbieter um die Bestandsdaten, die Rechnungsdaten oder die elektronischen Handelsdaten seiner Kunden ersuchen, wenn das FBI dem Anbieter schriftlich bestätigt, dass die ersuchten Daten für eine berechtigte Untersuchung zum Schutz gegen internationalen Terrorismus oder illegale Geheimdienstaktivitäten relevant sind und wenn eine solche Untersuchung einer Person aus den Vereinigten Staaten nicht allein auf der Grundlage von Aktivitäten erfolgt, die durch den ersten Verfassungszusatz geschützt sind. Der Telekommunikationsanbieter muss der Anfrage dann auch ohne eine gerichtliche Anordnung nachkommen.[585] Die Anfrage des FBI kann auf Antrag des Ersuchten von einem Gericht überprüft werden. Das Gericht kann das Ersuchen ändern oder aufheben, wenn die Auskunft auf Anfrage unbegründet, unterdrückerisch oder rechtswidrig ist.[586] Die Datenerhebung anlässlich der Terrorabwehr unterliegt weniger Einschränkungen als die zur Strafverfolgung.

584 Da sich sowohl die Datenspeicherungspraxis der amerikanischen Geheimdienste als auch die deutsche Vorratsdatenspeicherung aus dem Anlass der Terrorabwehr entwickelt haben und in Bereichen der Geheimdienste und der Strafverfolgung bewegen, ist zudem die Datenspeicherungspraxis im Rahmen der Geheimdienste erwähnenswert.

585 18 U. S. C. § 2709.

586 18 U. S. C. § 3511 (a).

c) Löschungspflicht

Anstatt der Bestimmung der pflichtgemäßen Löschung der durch den Diensteanbieter gespeicherten Daten – was bei fast keinem Datenschutzgesetz im Privatsektor eine konsequente Folge sein kann – wird die maximale Frist der Datenspeicherung, die die berechtigten Stellen vom Diensteanbieter fordern dürfen, gesetzlich eingeschränkt. Die Kommunikationsdatenanfrage ist im 18. U. S. C. § 2703 (f) geregelt. Danach kann jede staatliche Behörde die Telekommunikationsunternehmen oder die Internet Service Provider anweisen, noch vorhandene und künftig anfallende Kommunikationsdaten für einen Zeitraum von bis zu neunzig Tagen zu speichern. Die Speicherdauer kann nur einmalig um weitere neunzig Tage verlängert werden. Da es fast keine datenschutzrechtlichen Regelungen für die private Datenspeicherungspraxis und auch keine Regelung für die Löschungspflicht gibt, lassen sich die Speicherung und die Löschung der Daten kaum kontrollieren. Die Speicherdauer von neunzig Tagen – gegebenenfalls um weitere neunzig Tage – stellt ausschließlich die Speicherung der angeforderten Daten in diesem Zeitraum sicher, aber nicht ihre Löschung. Die Speicherungspraxis ist nicht an eine gesetzliche Löschungspflicht gebunden, sondern unterliegt der Marktautonomie. In Anbetracht des geltenden Gesetzes bewahren die meisten Internetdienstanbieter in den USA Daten mindestens dreißig bis neunzig Tage lang auf.[587] Die Internetdienstanbieter vernichten häufig die Daten, die für geschäftliche Zwecke wie Netzwerküberwachung, Betrugsprävention oder Abrechnungsstreitigkeiten nicht mehr erforderlich sind.[588] Nach US-amerikanischem Recht sind die Internetdienstanbieter jedoch nicht dazu verpflichtet, diese Daten innerhalb eines bestimmten Zeitraums zu vernichten. Die Löschungsvorschriften zahlreicher Einzelstaaten fordern ausschließlich, dass ein Unternehmen die personenbezogenen Daten dann sicher und effektiv vernichten muss, wenn es die Daten nicht mehr aufbewahren *will*. Darüber hinaus gibt es keine Löschungs- oder Übermittlungsverbotsvorschriften für bereits an die Ermittlungsbehörden übermittelte Daten.

587 *Ringland*, The European Union's Data Retention Directive and the United States's Data Preservation Laws: Finding the Better Model, 5 Shidler J. L. Com. & Tech. 13, 2009; *McCullagh*, Gonzales Pressures ISPs on Data Retention, ZDNET News v. 27. Mai 2006, abrufbar unter: https://www.zdnet.com/article/gonzales-pressures-isps-on-data-retention/.

588 *Swartz/Johnson*, U. S. asks Internet Firms to Save Data, NEWSWATCH v. 1. Juni 2006, abrufbar unter: https://newswatch.write2kill.in/news/2006/06/01/us-asks-internet-firms-to-save-data.

Der Privacy Act beschränkt die Übermittlung der Daten nur durch die Bestimmung, dass keine Behörde ihre Daten ohne schriftliche Aufforderung oder Einverständniserklärung der Betroffenen an eine andere Person oder Behörde weitergeben darf.[589] Hier bestehen jedoch keine spezifischen Erklärungen über den Begriff der anderen Behörden und keine Einschränkungen bezüglich der Datenverwendung zu anderen Zwecken innerhalb derselben Behörden. Für die hier genannten anderen Behörden gibt es keinen spezifischen Geltungsbereich und keine Beschränkungen für die Verwendung der Daten zu anderen Zwecken.

Auch für den Einsatz eines Geräts zum Erhalt der künftigen Verkehrsdaten ist die Verwendungsdauer gesetzlich bestimmt. Das *Pen Register Device* oder das *Trap and Trace Device* darf für einen Zeitraum von höchstens sechzig Tagen eingesetzt werden, und seine Einsatzdauer kann nur einmalig um weitere sechzig Tage verlängert werden.[590] Die Verlängerung kann nur mit einer gerichtlichen Anordnung auf Antrag der Staatsanwaltschaft gewährt werden. Für den Verlängerungsantrag genügt – genau wie für den Antrag auf eine erstmalige Anordnung – eine Bescheinigung, die besagt, dass die Daten, die möglicherweise durch eine Installation oder Verwendung eines solchen Geräts erhalten werden, für eine laufende strafrechtliche Untersuchung relevant sind. Nach Ablauf des ermächtigten Zeitraums wird das eingesetzte Gerät deinstalliert.

Ein Problem liegt aber bei den Daten, die entweder mit der Befugnis gemäß § 2703 ff. oder mit dem Einsatz eines Geräts nach § 3121 ff. schon von einem Telekommunikationsunternehmen an die Strafverfolgungsbehörden übermittelt wurden. Die Verarbeitung und die Löschung der schon übermittelten und damit der Kontrolle der Strafverfolgungsbehörden unterliegenden Daten sind gesetzlich nicht geregelt. Das ECPA beinhaltet also keine Regelung darüber, bis wann und wie die von einem Telekommunikationsunternehmen erhaltenen und damit bei einer anfragenden Stelle liegenden Daten nach der Verwendung gelöscht werden sollen.

d) Mitteilungspflicht

Die Benachrichtigungspflicht gilt nur für die Erhebung von Kommunikationsinhalten mit einer *subpoena* oder einer erleichterten Anordnung. Das

589 5 U. S. C. § 552a (b).
590 18 U. S. C. § 3123 (c) (1) und (2).

heißt, selbst wenn die Kommunikationsinhalte erlangt werden, besteht keine Mitteilungspflicht, soweit dies mit einer normalen Anordnung, also einem *warrant*, erfolgt. Die Mitteilungspflicht kann für einen Zeitraum von höchstens neunzig Tagen zurückgestellt werden, wenn das Gericht feststellt, dass ein Grund zur Annahme besteht, dass die Benachrichtigung über das Vorliegen einer gerichtlichen Anordnung nachteilig sein kann: wenn die Gefährdung des Lebens oder der körperlichen Sicherheit einer Person, die Flucht vor der Strafverfolgung, die Vernichtung oder die Manipulation von Beweisen oder die Einschüchterung potenzieller Zeugen droht oder wenn andernfalls ernsthaft eine Untersuchung gefährdet wird oder sich eine Verhandlung unnötig verzögert.[591]

Die Benachrichtigung ist aber nicht erforderlich für die Erhebung von Verkehrsdaten. Bei der Erhebung von Kommunikationsdaten nach § 2703 (c) oder nach § 3121 ff. entsteht keine Mitteilungspflicht. Bei der Datenerhebung nach § 2709 kann das FBI sogar das Offenlegungsverbot der Anfrage durch den Anbieter anfordern, wenn es versichert, dass das Fehlen eines Offenlegungsverbots zu einer Gefahr für die nationale Sicherheit der Vereinigten Staaten, zu einer Störung der strafverfolgenden oder geheimdienstlichen Ermittlungen, zu einer Störung der diplomatischen Beziehungen oder zu einer Gefahr für das Leben oder die körperliche Sicherheit einer Person führen kann.[592]

Der Rechtsschutz setzt die Kenntnisnahme des von einer staatlichen Maßnahme Betroffenen voraus. Die staatliche Behörde besitzt und verwendet hier jedoch die Kommunikationsdaten des Betroffenen, ohne dass er von dieser Maßnahme weiß. Doch unter dem Umstand, dass der Betroffene nicht davon weiß, kann der Schutz gegen eine unbefugte oder unbeschränkte Erhebung, Speicherung, Verwendung und Weitergabe von Kommunikationsdaten unmöglich gewährleistet werden.

591 18 U. S. C. § 2703 (b) (1) (B) und § 2705 (a) (1) und (2).
592 18 U. S. C. § 2709.

Teil 4: Rechtsvergleichung

A. Der verfassungsrechtliche Datenschutz in den einzelnen Rechtsordnungen

I. Deutschland

1. Privatsphären- und Datenschutz

a) Privatsphärenschutz

In der deutschen Verfassung lässt sich das Recht auf Privatsphärenschutz nicht ausdrücklich vorfinden. Trotzdem werden die verschiedenen Aspekte und Bereiche, die in der privaten Lebensführung eine wichtige Rolle spielen, spezifisch und subsidiär umfassend geschützt. Dazu gehört das Recht auf die Unverletzlichkeit der Wohnung aus Art. 13 GG, das Recht auf das Brief-, Post- sowie Fernmeldegeheimnis aus Art. 10 GG und das allgemeine Persönlichkeitsrecht aus Art. 2. Abs. 1 i. V. m. Art. 1 Abs. 1 GG. Mit diesen Grundrechten werden die konkreten Aspekte der Privatsphäre des Einzelnen einschließlich der Wohnung und des Fernmeldegeheimnisses geschützt.

Zum Schutz vor dem Eingriff in die Privatsphäre der Bürger als einen der wesentlichen Bestandteile des verfassungsrechtlichen Persönlichkeitsschutzes hat der Bundesgerichtshof in der Leserbrief-Entscheidung im Rahmen der Zivilrechtsprechung erstmals das allgemeine Persönlichkeitsrecht als ein verfassungsmäßig gewährleistetes Grundrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 anerkannt. Damit wird dem Einzelnen ein räumlich und thematisch bestimmter Bereich garantiert, der grundsätzlich frei von unerwünschter staatlicher Einsichtnahme bleiben soll. Aus dem allgemeinen Persönlichkeitsrecht hat die Rechtsprechung die verschiedenen Ausprägungen der Privatsphäre entwickelt: das Recht auf sexuelle Selbstbestimmung, das Recht auf individuelle Selbstbestimmung, das Recht auf wirtschaftliche Selbstbestimmung, das Recht am eigenen Wort, das Recht auf Selbstdarstellung, das Recht an der eigenen Wohnung und das Recht an den eigenen Daten. Außerdem hat die Rechtsprechung eine Möglichkeit eröffnet, um den Einzelnen auch gegen neuartige Gefährdungen der freien Persönlichkeitsentfaltung zu schützen, indem sie den Schutzbereich des allgemeinen Persönlichkeitsrechts nicht abschließend definiert hat.

b) Die Bedeutung des Datenschutzes für den Privatsphärenschutz

In der deutschen Verfassung ist auch das Recht auf Datenschutz nicht ausdrücklich genannt. Der Privatsphärenschutz sieht sich jedoch aufgrund des modernen technischen Fortschritts mit neuen Herausforderungen konfrontiert. Die automatisierte Datenverarbeitung eröffnet die Möglichkeit, personenbezogene Daten schnell miteinander zu verknüpfen, zu übermitteln und in neue Zusammenhänge zu bringen. Der moderne Fortschritt der Datenverarbeitung erfordert ferner – über den Schutz von Wohnung und Fernmeldegeheimnis und das allgemeine Persönlichkeitsrecht hinaus, das von der Rechtsprechung entwickelt und konkretisiert wird – den Schutz der selbstständigen Herrschaft über personenbezogene Daten. Einen neuen Horizont für den Umgang mit der neuen Rechtsmaterie des Datenschutzes hat das Volkszählungsurteil des Bundesverfassungsgerichts gesetzt. In diesem Urteil hat das Bundesverfassungsgericht die Grundrechtsberührung der Informationsverarbeitung anerkannt, das Grundrecht auf informationelle Selbstbestimmung als einen weiteren spezifischen Aspekt der Privatsphäre aus Art 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitet und einige wichtige Schlüsse daraus gezogen.

Das Bundesverfassungsgericht erkennt das Potenzial der Gefährdung der freien Persönlichkeitsentfaltung, das den Möglichkeiten der modernen Datenverarbeitung innewohnt, wobei es das Recht auf informationelle Selbstbestimmung als eine Ausprägung des allgemeinen Persönlichkeitsrechts wahrgenommen hat, das den Einzelnen gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten schützt. Das heißt, das Bundesverfassungsgericht erkennt die Notwendigkeit des Datenschutzes als einen weiteren Aspekt des Privatsphärenschutzes an und präzisiert nicht nur das allgemeine Persönlichkeitsrecht aus der Perspektive des Datenschutzes, sondern arbeitet daraus auch das Recht auf informationelle Selbstbestimmung heraus. Außerdem entwickelt das Bundesverfassungsgericht das Recht auf Gewährleistung der Vertraulichkeit und der Integrität informationstechnischer Systeme.

c) Der verfassungsrechtliche Datenschutz

Das Recht auf informationelle Selbstbestimmung, das das Bundesverfassungsgericht unter dem Aspekt des Datenschutzes aus dem allgemeinen Persönlichkeitsrecht abgeleitet hat, gibt dem Einzelnen die Befugnis, grundsätzlich selbst über die Preisgabe und Verwendung seiner personen-

bezogenen Daten zu bestimmen.[593] Das Gericht erkennt damit die Notwendigkeit des Schutzes dieser Befugnis unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung an. Diese Anerkennung beruht auf den folgenden Erkenntnissen:

1. Die freie Entfaltung der Persönlichkeit setzt den Schutz des Einzelnen gegen die unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten voraus.
2. Die Bürger sind mit den Einzelheiten der Datenverarbeitungsvorgänge unter den modernen Datenverarbeitungsbedingungen nicht vertraut. Die automatische Datenverarbeitung ermöglicht es, personenbezogene Daten unbegrenzt zu speichern und jederzeit in Sekundenschnelle abzurufen. Außerdem können die personenbezogenen Daten mit anderen Datensammlungen zu einem teilweisen oder weitgehend vollständigen Persönlichkeitsbild zusammengefügt werden.
3. Unter den Bedingungen der automatischen Datenverarbeitung gibt es kein belangloses Datum, da ein im Grunde belangloses Datum durch die der Informationstechnologie eigenen Verarbeitungs- und Verknüpfungsmöglichkeiten einen neuen Stellenwert erhalten kann.
4. Die Furcht vor einer unkontrollierbaren Persönlichkeitserfassung kann die Freiheit des Einzelnen, aus eigener Selbstbestimmung zu planen oder zu entscheiden, wesentlich einschränken.

Das Bundesverfassungsgericht entschied, den neuen Gefährdungen der Privatsphäre durch die automatisierte Datenverarbeitung mit Hilfe des Rechts auf informationelle Selbstbestimmung wirksam entgegenzutreten. In diesem Zusammenhang hat das Bundesverfassungsgericht einige Anforderungen an Eingriffe in das Recht auf informationelle Selbstbestimmung gestellt: Gesetzesvorbehalt, Normenklarheitsgebot, Verhältnismäßigkeitsgrundsatz, Zweckbindungsgrundsatz sowie Forderung nach organisatorischen und verfahrensrechtlichen Vorkehrungen zur Sicherung des Rechts auf informationelle Selbstbestimmung. Damit wurden einheitliche Grundsätze als ein Prüfungsstab für jeden Eingriff in personenbezogene Daten geschaffen.

Neben dem Datenschutz durch das Recht auf informationelle Selbstbestimmung hat das Bundesverfassungsgericht mit seinem Online-Durchsuchungsurteil auch durch ein verfassungsrechtlich neues Grundrecht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme als eine weitere Ausprägung des allgemeinen Persönlich-

593 BVerfGE 120, 274 (312); BVerfGE 65, 1 (43).

keitsrechts auf den Datenschutz gezielt. Mit diesem IT-Grundrecht wird seitens des Bundesverfassungsgerichts der Versuch unternommen, die Lücken im Datenschutz zu schließen. Diese bestehen bezüglich der möglichen Infiltration gesamter informationstechnischer Systeme, die sich außerhalb einer Wohnung befinden, und bezüglich solcher Daten, die nach Anschluss eines Kommunikationsprozesses nicht mehr von Art. 10 GG gedeckt sind und mangels einzelner, punktueller Datenerhebungen auch nicht oder nicht ausreichend dem Recht auf informationelle Selbstbestimmung unterliegen. Abgesehen von der Frage, ob das Recht auf Gewährleistung der Vertraulichkeit und Integrität informationstechnischer Systeme um den besonderen Schutz der Freiheit der Bürger willen erforderlich oder effektiv ist, lässt sich aus der Ableitung dieses Rechts von der Rechtsprechung feststellen, dass deutsche Recht das ausgeprägte Persönlichkeitsgefährdungspotenzial der modernen Datenverarbeitung wahrnimmt und gegen dieses Potenzial einen noch wirksameren Schutz der personenbezogenen Daten zu gewähren beabsichtigt. Die Position der Rechtsprechung gewinnt eine größere Bedeutung in Deutschland, wo sich unter der generellen Idee der Schutzpflicht des Staates auch eine Pflicht des Staates abzeichnet, aktive Maßnahmen zum Schutz der Privatsphäre von Individuen zu ergreifen.

2. Das einfachgesetzliche Datenschutzsystem

Im Sinne eines einheitlichen und umfassenden Datenschutzes erließ der Gesetzgeber in Deutschland im Jahr 1977 das Bundesdatenschutzgesetz, das sowohl in der Bundesrepublik als auch in den einzelnen Ländern Anwendung findet. Das BDSG regelt zusammen mit den Datenschutzgesetzen der Länder und anderen bereichsspezifischen Regelungen den Umgang mit personenbezogenen Daten, die in Informations- und Kommunikationssystemen oder manuell verarbeitet werden. Jede Datenverarbeitung – Datenerhebung, -verarbeitung und -nutzung – im öffentlichen und nichtöffentlichen Sektor wird in diesem Gesetz geregelt, jedoch auf unterschiedliche Weise. In der deutschen Rechtsordnung ist die Verarbeitung personenbezogener Daten grundsätzlich verboten und daher nur auf Basis eines Erlaubnistatbestandes zulässig.

II. USA

1. Privacy Protection und Datenschutz

a) Privacy Protection

Das Recht auf *privacy* wird von der US-amerikanischen Rechtsprechung anerkannt und erweitert. Der Begriff „privacy" wird in der US-amerikanischen Verfassung jedoch nicht genannt. Vor allem im Hinblick auf die Vagheit der Bedeutung von *privacy* gab es vielfältige Versuche, den Begriff zu definieren. Den verfassungsrechtlichen Schutz des Rechts auf *privacy* anerkannte der Supreme Court aber erst mit der *Griswold*-Entscheidung. Anfangs wurde der verfassungsrechtliche Schutz dieses Rechts hauptsächlich im Kontext des vierten Verfassungszusatzes diskutiert. Ursprünglich wurde das Recht auf *privacy* nur gegen das materielle Betreten eines verfassungsrechtlich geschützten Raums verfassungsrechtlich geschützt.[594] Dementsprechend wurde kein verfassungsrechtlicher Schutz gegen die Überwachung von Telefonleitungen gewährt, solange kein physisches Betreten der Wohnung erfolgte.

Der technische Fortschritt und die ausdrückliche Anerkennung des Rechts auf *privacy* veranlassten den Supreme Court später jedoch dazu, seine Ansicht zu ändern. In der *Katz*-Entscheidung ersetzte der Supreme Court hinsichtlich des Schutzes des Rechts auf *privacy* das Kriterium des materiellen Betretens eines verfassungsrechtlich geschützten Raums durch das Kriterium einer begründeten Erwartung auf *privacy*. Gemäß der *Katz*-Prüfung wird im Rahmen der subjektiven Prüfung (*personal agency*) geprüft, ob der Einzelne eine Erwartung auf *privacy* hat, während im Rahmen der objektiven Prüfung herauszufinden ist, ob diese Erwartung gesellschaftlich als begründet anerkannt werden kann. Damit ist ein staatliches Handeln auch ohne physisches Betreten als ein Eingriff in das Recht auf *privacy* anzusehen, wenn eine begründete Erwartung auf *privacy* anerkannt wird. Jede Person genießt somit den verfassungsrechtlichen Schutz ihrer *privacy*, mit einigen Ausnahmen, wenn sie eine begründete Erwartung auf *privacy* hat. Für die Durchsuchung durch die Strafverfolgungsbehörden ist ein *warrant* erforderlich, der durch einen *probable cause* gestützt wird.

Angesichts des technischen Fortschritts stellt sich jedoch eine weitere Frage, und zwar, ob der Einzelne eine bestimmte Tätigkeit, die eine Erwartung auf *privacy* hat, ausüben kann, auch wenn er die eingesetzte neuartige

---

594 Olmstead v. United States, 277 U. S. 438 (457 f.).

Technologie nicht kennt. In diesem Zusammenhang hat der Supreme Court der *Katz*-Prüfung ein weiteres Kriterium hinzugefügt, nämlich die Gewöhnlichkeit der eingesetzten Technologie im Hinblick auf *personal agency*.

b) Die Bedeutung des Datenschutzes für die Privacy Protection

Aus den zahlreichen Versuchen, den Begriff der *privacy* zu definieren, können die informationelle Privatheit, die Privatheit der Kommunikation und die körperliche Privatheit als die Hauptelemente extrahiert werden. Allerdings lässt sich feststellen, dass das Recht auf *privacy* nicht abschließend bestimmt werden kann. Es besteht daher die Möglichkeit, dass den Begriffen „Privacy Protection" und „Datenschutz" in der US-amerikanischen Rechtsordnung mehr oder minder dieselbe Bedeutung zukommt. Zur vollständigen und sinnvollen Rechtsvergleichung wäre es daher erforderlich, den weiten Begriff der Privacy Protection auf die Unterkategorie des Datenschutzes zu reduzieren und diesen zu untersuchen. Dadurch soll der Schutz der informationellen Privatheit im Vordergrund stehen.

c) Der verfassungsrechtliche Datenschutz

Auch mit Bezug auf die informationelle Privatheit wendet der Supreme Court die Katz-Prüfung an. Wird eine begründete Erwartung auf *privacy* anerkannt, stellt ein staatliches Handeln einen Eingriff in die informationelle Privatheit dar.

Hiermit wurde u. a. das Recht anerkannt, Mitgliederlisten vor einer staatlichen Stelle geheim zu halten. Der Supreme Court hat den vierten Verfassungszusatz über lange Zeit hinweg sowohl im Hinblick auf personenbezogene Daten unter der Herrschaft Dritter oder auf Daten ohne Inhalt – z. B. Telefonnummern –[595] als auch im Hinblick auf Daten beschämender Natur[596] als unanwendbar angesehen. In Anlehnung an den Fall *Roe v. Wade* hat der Supreme Court jedoch Leitlinien zu den verfassungsrechtlich geschützten Informationen vorgelegt:

595 Smith v. Maryland, 442 U. S. 735 (742).
596 Paul v. Davis, 424 U. S. 693 (713).

1. Der Einzelne hat das Recht, die Offenlegung von persönlichen Angelegenheiten durch staatliche Akteure zu verhindern.
2. Mit diesem Recht ist eine Pflicht auf Seiten des Staates verbunden, die Informationen zu schützen, zu deren Preisgabe dieser den Einzelnen zwingt.
3. Informationen, die eng mit den *fundamental areas* verbunden sind, werden durch das Selbstbestimmungsrecht geschützt und rechtfertigen einen stärkeren Schutz des verfassungsrechtlichen Rechts auf informationelle Privatheit.

In einer grundsätzlichen Entscheidung im Hinblick auf das Recht auf informationelle Privatheit[597] hat der Supreme Court im Jahr 1965 festgestellt, dass das Recht auf *privacy* als „das individuelle Interesse an einer Vermeidung der Offenlegung persönlicher Angelegenheiten" zu verstehen sei. Damit wurde das Recht auf informationelle Privatheit und dessen verfassungsrechtlicher Schutz anerkannt. Dem entspricht die Nixon-Entscheidung. Trotz dieser Auslegung erhielt der Supreme Court die in den beiden Fällen jeweils angegriffene Verordnung und Regelung aufgrund einer Interessenabwägung aufrecht.

Nach der Bewertung der Circuit Courts haben die Entscheidungen des Supreme Courts zwar das Interesse des Einzelnen an einer Vermeidung der Offenlegung seiner persönlichen Angelegenheiten zum einen und zum anderen das Interesse an der Selbstbestimmung bei wichtigen Entscheidungen klar festgestellt, der Supreme Court habe jedoch keine nachvollziehbare Leitlinie vorgelegt, die auf Fälle anwendbar ist, welche die informationelle Privatheit betreffen. Die Circuit Courts entwickelten daher ihrerseits eine nützliche Abwägungsgleichung. Mit Hilfe dieser Abwägungsgleichung war die Vielzahl der Fälle bezüglich der informationellen Privatheit im Rahmen des Circuit Court entschieden.

Der Supreme Court beschäftigte sich in NASA v. Nelson im Jahr 2011 wieder mit dem Recht auf informationelle Privatheit. Er hat hier den verfassungsrechtlichen Schutz des Rechts auf informationelle Privatheit nur implizit anerkannt und aufgrund einer Abwägung festgestellt, dass die Hintergrundprüfung von der NASA das implizit anerkannte Recht nicht verletzt hat.

Daraus werden die folgenden Schwächen in der US-amerikanischen verfassungsrechtlichen Rechtsprechung zum Datenschutz ersichtlich:

---

597 Whalen v. Roe, 429 U. S. 589.

1. Das Recht auf *privacy* umfasst das individuelle Interesse an einer Vermeidung der Offenlegung persönlicher Angelegenheiten. Der Supreme Court gewährt lediglich vor der öffentlichen Bekanntgabe Schutz, jedoch nicht vor der unbegrenzten Datenerhebung, -speicherung, -nutzung und internen Übermittlung personenbezogener Daten innerhalb öffentlicher Stellen.
2. Der verfassungsrechtliche Schutz des Rechts auf informationelle Privatheit wird nur implizit, aber nicht ausdrücklich anerkannt.
3. Angesichts der Abwägungsgleichung der Circuit Courts werden die personenbezogenen Daten unterschiedlich, nämlich je nach Art ihrer Sensibilität, geschützt.
4. In der verfassungsrechtlichen Nachprüfung stellt sich lediglich die Frage, ob Sicherungsmaßnahmen vorgesehen sind, aber nicht, ob sie hinreichend sind, um die personenbezogenen Daten vor der unbegrenzten Erhebung, Speicherung, Nutzung und Weitergabe zu schützen.

Diese Schwächen werden insofern noch hervorgehoben, als es nach US-amerikanischer Dogmatik keine Vorstellung von einer Schutzpflicht des Staates gibt, aktive Maßnahmen zum Schutz der *privacy* von Individuen zu ergreifen, und weil daher die aus der US-Verfassung ableitbaren Rechte ausschließlich als Abwehrrechte gegenüber dem Staat zu verstehen sind.

2. Das einfachgesetzliche Datenschutzsystem

Es fehlt in den USA an einem umfassenden Auffangdatenschutzgesetz. Es gibt lediglich bereichsspezifische Gesetze, die nur bestimmte Fälle einer Datenverarbeitung regeln. Demnach stützen sich die USA im Rahmen des Datenschutzes auf einen Flickenteppich eng fokussierter sektoraler Gesetze und freiwilliger Selbstregulierung. Die Datenschutzgesetze können je nach Normadressaten in zwei Kategorien aufgeteilt werden: zum einen Datenschutz im öffentlichen Sektor, zum anderen Datenschutz im privaten Sektor.

Diesem bereichsspezifischen Regelungsansatz gemäß ist die Verarbeitung von personenbezogenen Daten grundsätzlich zulässig, sofern keine rechtliche Grundlage für das Verbot einer Verarbeitung oder kein bereichsspezifisches Gesetz, das die Verarbeitung einschränkt, besteht.[598]

598 *Schwartz*, Zur Architektonik des Datenschutzes in den USA, in: *Stern/Pfeifer/Hain*, Datenschutz im digitalen Zeitalter, S. 110.

Aufgrund der schieren Menge der einschlägigen Gesetze ist es unmöglich, diese alle übersichtlich darzustellen. Unter diesen Gesetzen besonders zu beachten ist jedoch der Privacy Act. Der Privacy Act[599] schützt als direkte gesetzgeberische Folge der sog. Watergate-Affäre die Privaten gegen hoheitliche Eingriffe in deren Privatsphäre. Der wesentliche Grundsatz des Privacy Act besteht darin, die Datensammlung soweit möglich bei der betroffenen Person durchzuführen.[600] Außerdem wird betroffenen Personen ein Recht auf Einsichtnahme und gegebenenfalls auf Berichtigung der über sie gesammelten Daten gewährt.[601] Der Privacy Act ist deshalb von so großer Bedeutung, weil er das erste gesamtstaatliche Gesetz zum Schutz Privater gegen hoheitliche Eingriffe in deren Privatsphäre war. Er findet allerdings nur bei Regierungsstellen der Bundesbehörden, nicht bei Regierungsstellen der einzelnen föderalen Staaten Anwendung.

Neben dem Schutz der Privatsphäre vor hoheitlichen Eingriffen dienen verschiedene weitere Normen zum Datenschutz für den privaten Bereich, etwa der Fair Credit Reporting Act und der Gramm-Leach-Billey-Act für Finanzdienstleister sowie der Electronic Communications Privacy Act und der Children's Online Privacy Protection Act im Bereich der Telekommunikation und der neuen Medien.

Wie bereits erwähnt, fehlt ein allgemeines und bereichsübergreifendes Gesetz zum Schutz personenbezogener Daten sowohl für den öffentlichen als auch für den privaten Sektor. Auch wenn es im öffentlichen Sektor ein gesamtstaatliches Gesetz gibt, ist dieser Schutz begrenzt.

III. Vergleich

1. Privatsphärenschutz

In den beiden Rechtsordnungen wird ein Recht auf Privatsphäre nicht ausdrücklich genannt. Während die Bedeutung der Privatsphäre in der deutschen Rechtsdogmatik relativ einheitlich zu verstehen ist, ist der Begriff der *privacy* in den USA je nach Kontext sehr unterschiedlich zu verstehen.

Zum Zweck des Privatsphärenschutzes werden in Deutschland verschiedene Aspekte und Bereiche, die eine bedeutungstragende Rolle im Privatsphärenschutz spielen, verfassungsrechtlich geschützt. Dem Schutz der

599 5 U. S. C. A. § 552a von 1974.
600 5 U. S. C. A. § 552a (e).
601 5 U. S. C. A. § 552a (d).

Privatsphäre dient neben den Freiheitsrechten aus Art. 13 und Art. 10 vor allem das allgemeine Persönlichkeitsrecht. Dieses Recht verpflichtet alle staatliche Gewalt, die private Sphäre der Grundrechtsträger als individuelle Handlungssphäre und Sphäre der Intimität zu schützen.[602] Mit diesem Recht werden vielfältige Ausprägungen der Privatsphäre geschützt. Die Reaktionen auf neuartige Herausforderungen der freien Persönlichkeitsentfaltung sind dadurch möglich, dass das allgemeine Persönlichkeitsrecht nicht abschließend definiert ist.

In den USA hingegen wurde das Recht auf *privacy* von der Rechtsprechung aus *penumbras* und *emanations* mehrerer Verfassungszusätze gefasst und hauptsächlich im Kontext des vierten Verfassungszusatzes diskutiert. Die *privacy protection* konzentrierte sich daher auf den verfassungsrechtlich geschützten Raum und das physische Betreten desselben. Verfassungsrechtlich nicht geschützter Raum oder der Einsatz von Technik ohne physisches Betreten des privaten Raums im buchstäblichen Sinne genoss hingegen keinen verfassungsrechtlichen Schutz im Sinne der *privacy*. Dieses relativ enge Verständnis der *privacy protection* erfuhr mit dem neuen Kriterium einer begründeten Erwartung auf *privacy* nach der *Katz*-Entscheidung eine erhebliche Erweiterung. Weist der Einzelne eine Erwartung auf *privacy* auf und kann die Erwartung als gesellschaftlich betrachtet begründet angesehen werden, wird das Recht auf *privacy* anerkannt. Dadurch wurde die Entscheidung für die *privacy protection* mit Hilfe des Raums und des physischen Betretens aufgehoben. Der technische Fortschritt stellt jedoch eine neue Herausforderung bezüglich der Frage dar, ob der Einzelne eine Erwartung auf *privacy* aufweist. Der Supreme Court musste dabei die Schwierigkeit berücksichtigen, dass der Einzelne eine Erwartung auf *privacy* schafft, wenn die eingesetzte neuartige Technik allgemein nicht gewöhnlich ist. Die *privacy protection* in der US-amerikanischen Rechtsordnung wird somit durch die *Katz*-Prüfung und zusätzlich die Gewöhnlichkeit der eingesetzten Technik gewährt. Daraus lässt sich folgern, dass die US-Verfassung den Schutz des Privatlebens i. w. S. für einen engen, inneren und speziellen Bereich zumindest vor hoheitlichen Eingriffen garantiert. Damit wurde zwar der Rahmen festgelegt, der bestimmte Sphären von Privatheit garantiert, es sind dabei jedoch nur geringe Möglichkeiten gegeben, einen Schutz herbeizuführen, der alle Bereiche des Privatlebens umfasst.[603]

602 Vgl. *Kunig*, Grundgesetz-Kommentar, Art. 2 Rn. 32.
603 *Genz*, Datenschutz in Europa und den USA, S. 48.

2. Der verfassungsrechtliche Datenschutz

Durch zahlreiche Entscheidungen des Bundesverfassungsgerichts – z. B. seine Urteile zur Volkszählung, zur Vorratsdatenspeicherung und zur Online-Durchsuchung – ist in Deutschland ein starker verfassungsrechtlicher Datenschutz ohne Rücksicht auf die Sensibilität der Daten abgesichert. Das Bundesverfassungsgericht hat in seinem Volkszählungsurteil das allgemeine Persönlichkeitsrecht vor allem zu einem Recht auf informationelle Selbstbestimmung konkretisiert, damit der spezifische Datenschutz erfolgt. Im Zuge des Volkszählungsurteils hat das Bundesverfassungsgericht die Grundrechtsberührung der automatisierten Datenverarbeitung wahrgenommen und das Recht auf informationelle Selbstbestimmung entwickelt, um den Einzelnen gegen das der modernen Datenverarbeitung innewohnende Persönlichkeitsgefährdungspotenzial zu schützen. Das Recht ist als ein Anspruch des Einzelnen zu verstehen, die Bedingungen zu kontrollieren, unter denen personenbezogene Daten erlangt, übermittelt oder zur Nutzung gebraucht werden können. Durch dieses Verständnis des Rechts auf informationelle Selbstbestimmung wird der Schutz des Einzelnen vor der unbegrenzten Erhebung, Speicherung, Nutzung und Weitergabe seiner Daten unter den gegenwärtigen Datenverarbeitungsbedingungen garantiert. Neben der Ableitung dieses Rechts werden von der Rechtsprechung einige konkrete Anforderungen gestellt, um den materiellen Datenschutz zu verwirklichen. Zu diesen Anforderungen gehören der Gesetzesvorbehalt, das Normenklarheitsgebot, der Verhältnismäßigkeitsgrundsatz, der Zweckbindungsgrundsatz und die Forderung nach organisatorischen und verfahrensrechtlichen Vorkehrungen. Außerdem legt das Recht auf informationelle Selbstbestimmung dem Staat auch Schutzpflichten gegenüber Privaten auf.

Demgegenüber wird der Datenschutz in den USA unter dem Begriff „privacy" subsumiert, der nicht abschließend definiert werden kann.[604] Der Rahmen, der die bestimmten Bereiche des Rechts auf *privacy* garantiert, wird von der Rechtsprechung festgelegt. In Bezug auf das Recht auf informationelle Privatheit unter dem Recht auf *privacy* wird das Interesse des Einzelnen, die Offenlegung seiner persönlichen Angelegenheiten zu vermeiden, von der Rechtsprechung anerkannt und auf der Ebene der Circuit Courts wurde eine Abwägungsgleichung entwickelt. Jedoch betrifft dieser Rahmen lediglich den Schutz vor der öffentlichen Bekanntgabe von personenbezogenen Daten und gibt keine Garantie eines umfassenden

604 Vgl. *Genz*, Datenschutz in Europa und den USA, S. 39 m. w. N.

Rechts zur Datenkontrolle. Ein Recht des Einzelnen, seine Daten eigenständig zu kontrollieren, sprich die unbefugte oder übermäßige Erhebung, Speicherung, Nutzung und Weitergabe seiner Daten zu verhindern und selbst darüber zu entscheiden, ob, wann, wie und in welchem Maße seine Daten öffentlich bekannt gemacht werden, wird noch nicht wahrgenommen. Außerdem geht selbst dieser von der Rechtsprechung herausgearbeitete Schutz der informationellen Privatheit noch nicht über den Einzelfall hinaus.[605] Es gibt also keinen umfassenden Datenschutz, der dem Schutz durch das Recht auf informationelle Selbstbestimmung entspricht. Einen allgemeingültigen und verlässlichen Datenschutz kann der Einzelne in diesem Fall nicht erwarten. Wegen dieses Mangels an verfassungsrechtlicher Absicherung im Hinblick auf das Recht auf informationelle Privatheit kann ein bereichsübergreifender Privatsphären- und Datenschutz nicht erreicht werden.

Während der Datenschutz in Deutschland bereits grundrechtlich verankert ist, dieser den höchstgerichtlichen Schutz erfahren hat und die konkreten Anforderungen zum materiellen Datenschutz von der Rechtsprechung entwickelt wurden, scheint der US-amerikanische Datenschutz angesichts des Umstands, dass ein Recht auf informationelle Privatheit verfassungsrechtlich noch nicht umfassend abgesichert ist, noch einen weiten Weg vor sich zu haben.

3. Datenschutzsystem

Der Unterschied zwischen dem deutschen und dem US-amerikanischen Datenschutzrechtssystem beruht vor allem auf dem Datenschutzansatz. In Deutschland fungiert das BDSG als ein umfassendes Datenschutzgesetz, unter dem jede Datenverarbeitung grundsätzlich verboten ist, wenn es keinen gesetzlichen Erlaubnistatbestand gibt. In den USA hingegen wurde es vermieden, allgemeine Datenschutzgesetze und -vorschriften aufzustellen. Für diesen Zweck wurde eine bereichsspezifische Sondergesetzgebung mit einer Unterstützung der Selbstregulierung ausgewählt. Hier ist jede Datenverarbeitung grundsätzlich zulässig, soweit es gesetzlich nicht anders bestimmt ist.

Die rasch gewachsenen Möglichkeiten der elektronischen Datenverarbeitung machen einen umfassenden gesetzlichen Datenschutz erforderlich. Denn der sektorale Ansatz hinterlässt notwendigerweise eine Vielzahl

605 Vgl. *Genz*, Datenschutz in Europa und den USA, S. 49 m. w. N.

von wesentlichen Bereichen, in denen ein Schutz der informationellen Privatheit bzw. personenbezogener Daten nicht sichergestellt ist. Lediglich grundlegende Schranken- und Steuerungsmechanismen der Datenverarbeitung durch bereichsübergreifende Vorgaben zum Datenschutz können einen sicheren Rechtsschutz im Rahmen des Umgangs mit personenbezogenen Daten versprechen.

Das unterschiedliche Datenschutzniveau zwischen der EU und den USA hat zu einer Vereinbarung über die Grundsätze des sog. „sicheren Hafens" zwischen der EU und dem Handelsministerium (Department of Commerce) der USA geführt.[606] Den Ausgangspunkt für diese Vereinbarung bildet die EU-Datenschutzrichtlinie,[607] die die Mindeststandards für den Datenschutz beschreibt, die in allen Mitgliedstaaten der EU durch nationale Gesetze sichergestellt werden müssen, um den freien Verkehr personenbezogener Daten innerhalb der EU durch die Schaffung eines gleichen Datenschutzniveaus in allen EU-Mitgliedstaaten zu erleichtern. Die Richtlinie legt die Verpflichtungen für die Verarbeiter von personenbezogenen Daten und die Rechte für die Betroffenen fest. Gemäß der Richtlinie ist ein Datentransfer in Drittstaaten, die über kein mit dem EU-Recht vergleichbares Datenschutzniveau verfügen, verboten. Es wurde festgestellt, dass die USA kein angemessenes Schutzniveau bieten, da es dort keine umfassenden gesetzlichen Regelungen zum Datenschutz gibt, die dem europäischen Standard entsprechen. Allerdings sieht Art. 25 Abs. 6 der Richtlinie vor, dass die Kommission der Europäischen Gemeinschaft die Angemessenheit des Datenschutzes in einem Drittland feststellen kann, sprich, dass sie darüber befinden kann, ob ein Drittland hinsichtlich des Schutzes der Privatsphäre sowie der Freiheiten und Grundrechte von Personen ein angemessenes Schutzniveau im Sinne des Absatzes 2 gewährleistet oder nicht. In diesem Zusammenhang können sich Organisationen in den USA freiwillig darauf verständigen, die Safe-Harbor-Grundsätze

606 Safe Harbor, Kommissionsentscheidung 2000/520/EG: Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA.

607 Die Richtlinie 95/46/EG zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr. Die Richtlinie wurde ab dem 25. Mai 2018 durch die Verordnung (EU 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG) ersetzt.

einzuhalten, und diese Einhaltung öffentlich bestätigen. Dies führt zu der Annahme, dass diese Organisationen den Angemessenheitsstandard der EU-Richtlinie für den Datenschutz erfüllen. Infolgedessen kann der internationale Informationsaustausch zwischen Unternehmen in der EU und jenen Organisationen in den USA, die den Safe-Harbor-Bestimmungen entsprechen, stattfinden. Die Safe-Harbor-Vereinbarung enthält vor allem die folgenden Punkte: 1. Die Organisation muss Privatpersonen darüber informieren, zu welchem Zweck sie die Daten über die Personen erhebt und verwendet und wie die Personen die Organisation bei eventuellen Nachfragen oder Beschwerden kontaktieren können; 2. An wen dürfen die Daten weitergegeben werden und welche Mittel sowie Wege sollten die Daten den Privatpersonen zur Verfügung stellen, damit die Verwendung und Weitergabe der Daten eingeschränkt werden können?

B. Datenschutz bei den konkreten Maßnahmen in den einzelnen Rechtsordnungen

I. Strafregister

Die Daten aus dem Strafregister spielen in jeder Phase des Strafverfahrens eine bedeutsame Rolle. Unter den Bedingungen der modernen Datenverarbeitung sollte der Schutz der im Strafregister gespeicherten Daten in Bezug auf den Schutz der Privatsphäre als eines Teils des Rechts auf Freiheit des Einzelnen jedoch ebenfalls im Vordergrund stehen. Denn die Speicherung strafrechtlich relevanter Daten ist zwar im Interesse der Öffentlichkeit, die Strafregistrierungen für den Zweck zukünftiger Verbrechensermittlungen und gerichtlicher Entscheidungsfindungen beizubehalten, greift aber in das informationelle Selbstbestimmungsrecht des Betroffenen ein. Ein ehemaliger Verurteilter hat das Recht, sein Leben ohne das Stigma von Strafregistrierungen zu führen.

Im Folgenden sollen die Ausgestaltungen des Strafregistersystems in Deutschland und den USA übersichtlich dargestellt und die beiden Systeme im Hinblick auf die Organisationsstruktur, die Erhebung, die Speicherung, die Übermittlung und die Weitergabe von Daten unter dem Aspekt von Einschränkungen zum Zweck des Datenschutzes miteinander verglichen werden.

1. Deutschland

a) Organisationsstruktur

Das deutsche Strafregistersystem besteht aus dem BZR als einem einheitlichen Strafregister und dem ZStV. Die Einrichtung und die Führung der beiden Register werden vor allem durch §§ 474–495 StPO ermächtigt. Entscheidungen gegen Jugendliche werden gesondert in das Erziehungsregister eingetragen, das in das BZR integriert ist. Damit wird den Besonderheiten des Jugendstrafrechts und seinen vorwiegend auf erzieherische Wirkungen abstellenden Maßnahmen Rechnung getragen. Bezüglich der Organisationsstruktur sollen das Erhebungs-, Speicherungs- und Übermittlungsverfahren von Daten in den Registern übersichtlich vorgestellt werden.

Bei einem Erhebungsvorgang beim BZR übermittelt eine mitteilungspflichtige Stelle der Registerbehörde mittels Fernübertragung die in das Register einzutragenden Inhalte. Die mitteilungspflichtigen Stellen schreibt § 1 Abs. 1 BZRGVwV im Einzelnen vor, die in das Register einzutragenden Inhalte § 3 BZRG. Damit das Register aktuell gehalten wird, ist die Mitteilungspflicht mit obligatorischen Mitteilungsfristen verbunden. Die Übermittlung soll bei Entscheidungen binnen eines Monats nach Eintritt der Vollziehbarkeit, Unanfechtbarkeit oder Rechtskraft mitgeteilt werden. Die mitgeteilten Daten erfahren elektronisch zahlreiche Plausibilitätsprüfungen und eine Identitätsfeststellung und werden danach eingeordnet. Die Speicherung erfolgt erst zu diesem Zeitpunkt. Die im Register gespeicherten Daten werden mittels Datenübertragung angefragt und daraufhin übermittelt (Auskunftserteilung). Die Auskunftserteilung aus dem Register durch die Registerbehörde erfolgt entweder im Weg eines Führungszeugnisses oder einer unbeschränkten Auskunft. Bei dieser Stufe muss gewährleistet werden, dass ein unbefugter Zugriff Dritter auf die Daten wirksam abgewehrt wird und dass die dem jeweiligen Stand der Technik entsprechenden Maßnahmen zur Sicherstellung von Datenschutz und Datensicherheit – z. B. Verschlüsselungsverfahren im Falle der Nutzung allgemein zugänglicher Netze – getroffen werden.

Beim ZStV, das mit umfassenden und schnell verfügbaren Informationen über die bundesweit gegen einen Beschuldigten geführten Ermittlungs- und Strafverfahren der Staatsanwaltschaft zur Erleichterung der sachgerechten Führung eines Ermittlungsverfahrens eingerichtet wurde, lehnen sich die Erhebungs-, Speicherungs- und Übermittlungsverfahren teilweise an das Verfahren beim BZR an. Die Staatsanwaltschaften teilen

die einzutragenden Daten der Registerbehörde zu dem in § 492 Abs. 2 Satz 2 StPO genannten Zweck im Weg der Datenfernübertragung mit. Die einzutragenden Daten werden in § 492 Abs. 2 Satz 1 StPO und § 4 ZStVBetrV aufgeführt. Da dieser Regelungsbereich zum unmittelbaren Vorfeld des gerichtlichen Verfahrens gehört, wird die entsprechende Eintragung im ZStV automatisch gelöscht, wenn eine solche Entscheidung in das BZR eingetragen wird.[608] Eine Frist hierfür wird nicht festgelegt, auch wenn die ZStVBetrV vorschreibt, dass die Mitteilung erfolgen muss, sobald ein Strafverfahren anhängig wird. Mit diesen Informationen wird eine Vollspeicherung im Register erreicht. Die Datenübermittlung zur Anfrage und Auskunftserteilung erfolgt normalerweise per Datenfernübertragung. Die ZStVBetrV schränkt die Stellen ein, die eine Auskunft aus dem ZStV erhalten dürfen (ZStVBetrV § 6 Abs. 1 und 2).

b) Inhalt des Registers

Im BZRG werden die im BZR einzutragenden Daten ausführlich geregelt. Danach ist neben strafgerichtlichen Verurteilungen auch Weiteres im BZR zu speichern: strafgerichtliche Verurteilungen, Entscheidungen von Verwaltungsbehörden und Gerichten, Vermerke über Schuldunfähigkeit, gerichtliche Feststellungen nach § 17 Abs. 2, § 18 BZRG, nachträgliche Entscheidungen und Tatsachen und sogar strafgerichtliche Verurteilungen ausländischer Gerichte. Die Registeraufgabe wurde damit erheblich erweitert.[609] Das Eintragen von Entscheidungen und Anordnungen gegen Jugendliche regelt § 60 BZRG.

Die in das ZStV einzutragenden Daten regeln § 492 Abs. 2 StPO und § 4 ZStVBetrV. Danach sind nur die Personendaten der beschuldigten Person, die Daten zur Straftat, die Vorgangsdaten wie etwa die mitteilende Stelle, die sachbearbeitende Stelle der Polizei sowie die Aktenzeichen und die Daten zum Verfahrensstand zu speichern. Die Speicherung hängt nicht vom Gewicht der vorgeworfenen Taten ab, sondern es werden die Ermittlungsverfahrensdaten bezüglich aller beschuldigten Personen gespeichert.

608 *Gieg*, KK-StPO, § 494 Rn. 4.

609 In Bezug auf die erweiterte Aufgabe hat sich die Bezeichnung zutreffend von *Strafregister* zu *Bundeszentralregister* geändert (vgl. dazu oben Fn. 174).

c) Verwendung der Daten aus dem Register

Um die informationelle Selbstbestimmung des Einzelnen zu schützen, hat das Bundesverfassungsgericht in seinem Urteil vom 15. Dezember 1983[610] einige Anforderungen gestellt. Sie gelten auch für die Daten im Strafregister. Da bei der Verwendung der Daten aus dem Register stets die Gefahr besteht, dass hochsensible Daten wie etwa eine Verurteilung oder eine sonst eintragungspflichtige Tatsache gegen den Willen des Bestraften bekannt werden und diesem dadurch Nachteile entstehen, wird bei der Verwendung der Daten aus dem Register besondere Sorgfalt gefordert. Die Verwendung von Daten aus dem Strafregister wird deswegen unter verschiedenen Aspekten eingeschränkt.

Diejenigen, die Anfragen stellen und gegebenenfalls eine Auskunft aus dem Register erhalten dürfen, sind beim BZR nur der Betroffene – ausnahmsweise auch sein Vertreter oder auch die Behörde, wenn das Führungszeugnis zur Vorlage bei ihr vorgelegt wird – und die in § 41 BZRG genannten Stellen; beim ZStV sind es nur die in § 6 Abs. 1 und 2 ZStV-BetrV genannten Behörden. Das deutsche Strafregistersystem beschränkt also, wer Auskunft erhält.

Auskunft aus dem BZR kann entweder im Weg des Führungszeugnisses oder der unbeschränkten Auskunft erteilt werden. Je nach Auskunftsmöglichkeit gelten unterschiedliche Einschränkungen. Beim Führungszeugnis werden die Eintragungen im Register mit bestimmten Aufnahmenormen und -fristen verbunden. Die Aufnahmefristen richten sich nach der Höhe der Verurteilungen. Die Mitteilungspflicht an den Betroffenen wird in der Regel nicht vorgeschrieben, da ein Führungszeugnis grundsätzlich von ihm selbst beantragt wird. In das Führungszeugnis zur Vorlage bei einer Behörde hat die das Zeugnis erhaltende Behörde dem Antragsteller auf Verlangen Einsicht zu gewähren. Anders als beim Privatführungszeugnis unterliegt das Behördenführungszeugnis dem Zweckbindungsprinzip; es wird daher gefordert, dass die Behörde das Zeugnis zur Erledigung ihrer hoheitlichen Aufgaben benötigt (§ 31 Abs. 1 BZRG). Die Weitergabe von Führungszeugnissen hängt durchaus vom Willen des Betroffenen ab. Das Behördenführungszeugnis darf an eine andere Behörde weitergegeben werden, wenn der Betroffene damit einverstanden ist.

Die Situation ist eine andere, wenn es um unbeschränkte Auskünfte geht. In unbeschränkten Auskünften sind auch solche Eintragungen enthalten, die nicht in das Führungszeugnis aufgenommen werden. Die

610 BVerfGE 65, 1.

Eintragungen beeinflusst nur der Löschungsvorgang. Eine unbeschränkte Auskunft wird auf Ersuchen der berechtigten Stellen erteilt, ohne dass der Betroffene davon Kenntnis nimmt. Eine Person kann auf Antrag nur davon Kenntnis nehmen, welche Eintragungen über sie im Register enthalten sind. Man kann als Einzelner also nicht feststellen, ob irgendeine Behörde Auskunft über seine im Register gespeicherten Daten angefragt und danach erhalten hat. Die Zweckangabe wird bei einer Anfrage gesetzlich gefordert und die Zwecke werden je nach Behörde unterschiedlich aufgezählt, damit die Daten im Register vor dem übermäßigen Zugriff geschützt werden können – z. B. bei Anfragen von Gerichten, Gerichtsvorständen, Staatsanwaltschaften und Aufsichtsstellen für Zwecke der Rechtspflege. In einem Ersuchen muss also angegeben werden, aus welchem Grund eine Auskunft erforderlich ist, die dann auch ausschließlich zu dem genannten Zweck verwendet wird. Außerdem wird das Ersuchen grundsätzlich auf Einzelanfragen begrenzt. Unbeschränkte Auskünfte dürfen nur weitergegeben werden, wenn dies zur Vermeidung von Nachteilen für den Bund oder ein Land unerlässlich ist oder wenn andernfalls die Erfüllung öffentlicher Aufgaben erheblich gefährdet oder erschwert würde. Darüber hinaus werden die Auskünfte nur den mit der Entgegennahme oder Bearbeitung betrauten Bediensteten erteilt. Dadurch soll dem Betroffenen die weitestgehende Geheimhaltung seiner Daten garantiert werden.

Die anfragenden und gegebenenfalls Auskunft aus dem ZStV erhaltenden Stellen sind gesetzlich auf die Strafverfolgungsbehörden eingeschränkt.[611] Die Daten im ZStV unterliegen dem Zweckbindungsprinzip. Die Daten dürfen also nur zum Zweck der Verwendung im Strafverfahren gespeichert, verändert und verwendet werden. Die im ZStV gespeicherten Daten werden zum Zweck der Strafrechtspflege verwendet, genauso wie bei unbeschränkten Auskünften, ohne dass der Betroffene davon Kenntnis nimmt. Außerdem flankieren die erforderlichen und angemessenen Maßnahmen die Verwendung personenbezogener Daten in diesem Bereich, um die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der im Register gespeicherten Daten sicherzustellen.

611 Ausnahmsweise darf auch den Verfassungsschutzbehörden des Bundes und der Länder, dem Amt für den Militärischen Abschirmdienst und dem Bundesnachrichtendienst Auskunft erteilt werden, sofern diesen Stellen ein Auskunftsrecht gegenüber den Strafverfolgungsbehörden zusteht. Das dient dazu, unnötigen Aufwand zu vermeiden.

d) Speicherdauer

Wie oben erwähnt, bleiben Eintragungen im BZR grundsätzlich nicht dauerhaft gespeichert. Das Gesetz eröffnet neben der Nichtaufnahme einer Eintragung in das Führungszeugnis die Möglichkeit der Tilgung, um das Rehabilitationsinteresse des Betroffenen in Rechnung zu stellen. Neben der vollständigen Entfernung von Eintragungen aus dem BZR gemäß §§ 16 Abs. 2, 24 und 63 BZRG erfolgt eine Tilgung aufgrund Fristablaufs oder aufgrund Anordnung der Registerbehörde. Die Anordnungsmöglichkeit der Tilgung dient der Einzelfallgerechtigkeit, die bei der fristgebundenen Tilgung nicht berücksichtigt wird; damit wird sie auf wenige Ausnahmefälle begrenzt. Die Tilgung aufgrund einer Anordnung erfolgt auf Antrag oder von Amts wegen nach der Entscheidung der Registerbehörde.

Das BZRG regelt die Tilgungsfristen je nach Höhe der Hauptstrafe. Nach einem Tilgungsfristablauf werden die Daten von einem besonderen Löschprogramm automatisch gelöscht. Die zu tilgenden oder schon getilgten Daten dürfen mit einigen Ausnahmen (§ 52 BZRG) nicht mehr verwertet werden (Verwertungsverbot, § 51 BZRG); daher genießt der Betroffene das Schweigerecht im Hinblick auf seine getilgten Daten. Auch wenn die Tilgungsfristen noch nicht abgelaufen sind, kann in besonderen Fällen die Tilgung aufgrund Anordnung der Registerbehörde vorkommen. Die Fälle sieht § 49 BZRG vor. Darüber hinaus dürfen Entscheidungen aus dem Register fristunabhängig entfernt werden, wenn sie in einem Wiederaufnahmeverfahren rechtskräftig aufgehoben wurden. § 24 BZRG regelt noch eine andere fristunabhängige Tilgungsmöglichkeit, um einem stetigen Anwachsen des Registers durch Belassen überholter Eintragungen entgegenzuwirken.[612] Amtsgerichte, Anstaltsleitungen oder amtliche Vertretungen der Bundesrepublik Deutschland müssen die Registerauszüge, die zur Einsichtnahme des Betroffenen gemäß § 42 BZRG herangezogen wurden, nach Einsichtnahme vernichten.

Die Speicherung bleibt grundsätzlich unberührt, bis die Eintragungen im ZStV in das BZR übernommen werden. § 494 StPO regelt die Ausnahmefälle: die versehentliche Eintragung der Daten, Doppelspeicherungen, den rechtskräftigen Freispruch, die unanfechtbare Ablehnung der Eröffnung des Hauptverfahrens, Verfahrenseinstellungen, die nicht nur vorläufig oder endgültig sind, und ein weiteres Verfahren zur Eintragung in das ZStV. Außerdem ist es gesetzlich vorgesehen, dass die ersuchende Stelle nach erfolgter Identifizierung alle übermittelten Daten, die sich nicht auf

612 *Tolzmann*, Bundeszentralregistergesetz, § 24 Rn. 4.

den Betroffenen beziehen, unverzüglich zu löschen hat; dies gilt auch bei einer unmöglichen Identifizierung.

Die im ZStV gespeicherten Daten werden nicht nur gelöscht, sondern unter bestimmten Umständen auch gesperrt. § 494 Abs. 3 i. V. m. § 489 Abs. 7 und 8 StPO führen die hierfür relevanten Umstände auf. Die Verwendung der gesperrten Daten beschränkt sich nur auf die Verwendung zu dem Zweck, für den die Löschung unterblieben ist, und auch soweit dies zur Behebung einer bestehenden Beweisnot unerlässlich ist.

2. USA

a) Organisationsstruktur

In den USA steht kein national zentralisiertes Strafregister, sondern das dezentralisierte III-System zur Verfügung, das ein zwischenstaatliches Computernetzwerk zum Datenaustausch zwischen dem Bund und den Einzelstaaten im Hinblick auf die Strafregistrierungen ist. Jeder Staat und auch das FBI (bezüglich bundesgesetzlicher Verbrechen) betreiben jeweils ihr eigenes Strafregister, die mittels des III-Systems durch einen Index-Pointer-Ansatz miteinander vernetzt sind. Das III-System wird vom NCIC beim FBI geführt. Das III-System gibt auf Ersuchen an, ob eine Person irgendwo im Land bereits registriert ist: falls ja, verweist der *Interstate Identification Index* die anfragende Behörde an das FBI und/oder an ein oder mehrere der staatlichen Register, die den ersuchten Datenbestand erhalten.

Die im Strafregister einzutragenden Daten werden zuerst im Strafregister desjenigen Staates erhoben und gespeichert, in dem ein Verbrechen strafverfolgend ermittelt und in dem gerichtliche Entscheidungen gegen den Betroffenen getroffen wurden. Der methodische Unterschied zwischen am NFF teilnehmenden Staaten und daran nicht teilnehmenden Staaten liegt innerhalb des III-Systems darin, die in eigenen Strafregistern gespeicherten Daten dem FBI mitzuteilen. Erstere senden dem FBI nur die ersten Registrierungsdaten (Fingerabdrücke und Identifikationsdaten) über jede Person, um den Index des III-Systems zu aktualisieren. Die Staaten speichern die anderen im Strafregister einzutragenden Daten immer wieder in ihrem eigenen Strafregister. Die Daten stehen für eventuelle Anfragen aus anderen Einzelstaaten oder aus zugelassenen Bundesbehörden zur Verfügung. Die nicht am NFF teilnehmenden Staaten leiten demgegenüber alle Strafregistrierungen an das FBI weiter. Mit allen mitgeteilten

Daten wird die Speicherung im NFF und zugleich die Aktualisierung des Index erreicht.

Die Regelungen des Zugangs zu den Daten und der Auskunftserteilung von Daten aus dem Register sind zwar von Staat zu Staat unterschiedlich, das Anfrage- und Auskunftsverfahren unter dem III-System läuft jedoch insgesamt ähnlich ab. Eine Anfrage über eine Person wird zunächst über das staatliche Telekommunikationsnetz an das staatliche Repository gestellt. Das staatliche Strafregister leitet die Anfrage dann über das NCIC-Netzwerk an den III-Computer weiter, der daraufhin die anfragende Behörde an das FBI und/oder an ein oder mehrere der staatlichen Strafregister verweist, von denen Strafregistrierungen über die Person erhalten werden. Das anfragende staatliche Strafregister kann die Daten mit Hilfe des NCIC-Netzwerks oder des *National Law Enforcement Telecommunications Systems* (NLETS-Netzwerk) direkt aus den angegebenen Quellen erhalten. Das Strafregister übermittelt die Antwort an die anfragende Behörde. Bei der Weitergabe, der Löschung sowie der Vernichtung der einmal angebotenen Antwort gilt keine Regelung oder Einschränkung.

b) Inhalt des Registers

Was in die staatlichen Strafregister eingetragen werden soll, ist nicht bundesgesetzlich geregelt. Über die in das Register einzutragenden Daten besteht keine Einigkeit zwischen den Einzelstaaten. Das führt dazu, dass Daten in einem Staat gespeichert, in einem anderen hingegen nicht gespeichert werden. Der Begriff der *criminal history records* umfasste ursprünglich nicht nur die strafgerichtlichen Verurteilungsdaten, sondern auch die Verhaftungsdaten, also auch die Strafverfahrensdaten ohne Verurteilung.

Unabhängig davon, was in einem staatlichen Strafregister registriert werden soll, ist der Datenaustausch unter dem III-System bundesgesetzlich geregelt. Zum einen erfolgt die Mitteilung der Strafregistrierung unter dem III-System nur für schwere und/oder erhebliche (*serious and/or significant*) Erwachsenen- und Jugendstraftaten.[613] Auch wenn auf staatlicher Ebene eine Datenspeicherung für minder schwere Straftaten erreicht wird, können die Daten nicht durch eine Suche des III-Systems herausgefunden werden. Zum anderen erfährt die Datenspeicherpraxis eine tendenziell allmähliche Erweiterung. Dies gilt insbesondere für Entscheidungen gegen Jugendliche. Die Daten für schwere Straftaten durch Jugendliche werden

613 28 C. F. R. § 20.32 (a).

deswegen nun in staatlichen Strafregistern gespeichert. Bei den *criminal history records* handelt es sich um Informationen, die von Strafverfolgungsbehörden über Personen gesammelt werden und die aus identifizierbaren Beschreibungen und Feststellungen von Verhaftungen, Festnahmen, Anklageschriften oder anderen formellen Strafanzeigen einschließlich daraus resultierender Freisprüche, Verurteilungen oder Strafvollzugskontrollen bestehen.[614] Dabei werden für Identifizierungsdaten normalerweise Name, Adresse, Geburtsdatum, Sozialversicherungsnummer, Geschlecht, Rasse, physikalische Eigenschaften wie Haar- und Augenfarbe, Größe, Gewicht und alle auffälligen Narben, Marken, Tattoos oder auch Fingerabdrücke und für Dispositionsdaten die Daten über alle Entscheidungen über Personen gespeichert.

c) Verwendung der Daten aus dem Register

Wer berechtigt ist, die Strafregistrierungen bei einer Registerbehörde zu ersuchen und daraus Auskunft zu erhalten, regelt 42 U. S. C. § 14616 IV (b) und 20 C. F. R. § 20.21 (b) und § 20.33 (a). Dort ist jede Auskunft zweckgebunden. Danach stehen die Strafregistrierungen sowohl den Strafverfolgungsbehörden als auch anderen Behörden für nichtstrafrechtliche Zwecke zur Verfügung, für die das Bundes-, Bundesordnungs- oder Staatsgesetz erlaubt, die nationalen Indexprüfungen zu verwenden. Darüber hinaus kann der Betroffene eine Kopie eines im Strafregister eingetragenen Datensatzes gegen eine Gebühr in Höhe von 18 USD erhalten, um es einzusehen oder inhaltlich zu ändern, korrigieren oder aktuell zu halten.[615] Diese Einschränkung der Personen, die zum Zugriff auf die Strafregistrierungen berechtigt sind, ist aus drei Gründen in der Wirksamkeit begrenzt. Erstens ist es in den USA zulässig, dass Arbeitgeber eine Hintergrundprüfung[616] über Arbeitsbewerber nur mit deren Zustimmung vornehmen.[617] Eine Studie der *Society for Human Resource Management* zeigte aber, dass

614 42 U. S. C. § 14616 *Overview* (b) (4) (A).

615 28 C. F. R. § 16.30 bis 34.

616 Eine Hintergrundprüfung umfasst eine Überprüfung der Geschäfts-, Straf-, Beschäftigungs- und/oder Finanzdaten einer Person.

617 Wenn Arbeitgeber unter der *third-party-doctrine* eine Hintergrundprüfung (einschließlich Kredit-, Straf- und Vergangenheitsarbeitgeberprüfungen) durchführen, wird diese durch den Fair Credit Reporting Act von 1970 (FCRA) abgedeckt. Ungefähr 30 Prozent der Arbeitgeber führen eine offizielle Hintergrundprüfung von Bewerbern durch und etwas weniger als die Hälfte aller Arbeitge-

in der Realität mehr als 80 Prozent der amerikanischen Arbeitgeber kriminalpolizeiliche Überprüfungen potenzieller Mitarbeiter durchführen.[618] Es gibt ferner private Informationsdienstunternehmen, die gegen eine geringe Gebühr eine Internetsuche nach Strafregistern zu den kriminalpolizeilichen Überprüfungen anbieten. Diese Unternehmen sind in gewissem Umfang durch den Fair Credit Reporting Act *(FCRA)* geregelt. Staatliche Gesetze regeln diese Unternehmen jedoch nicht direkt, sondern verbieten Arbeitgebern nur, Strafregistrierungen in Arbeitsentscheidungen zu verwenden.[619] Einen zweiten Grund bilden die bei den Gerichten gespeicherten und von diesen geführten Daten, die durch das E-Government-Gesetz von 2002 öffentlich leicht zugänglich geworden sind. Einen dritten Anlass zum Zweifel an der Wirksamkeit geben die sogenannten Megans Gesetze, die die Identitäten, Adressen und Straftaten von Sexualstraftätern über das Internet öffentlich zugänglich machen. Diese Gesetze führen dazu, dass jeder die Daten von Sexualstraftätern erhalten kann.

Das Anfrage- und Auskunftsverfahren läuft meist online über spezielle Computer-Terminals ab. Dabei wird gesetzlich gefordert, dass ein Verfahren verfügbar ist, das die Genauigkeit und die Vertraulichkeit der Daten schützt und das sicherstellt, dass die Daten nur von den Berechtigten für berechtigte Zwecke verwendet werden und dass die Abfragen grundsätzlich auf Einzelanfragen begrenzt sind.[620] Aber die Einzelheiten werden den einzelnen Staaten überlassen. Um einen unbefugten oder übermäßigen Zugriff auf Strafregistrierungen zu vermeiden, wird teilweise in den Gesetzen aller oder einiger Staaten vorausgesetzt, eine Übermittlung von Daten im Strafregister an bestimmte im Gesetz vorgeschriebene Zwecke zu binden – eine Weitergabe von Daten an eine andere als die anfragende Behörde ist zwar möglich, aber nur innerhalb des angefragten Zwecks. Im Falle der Übermittlung von *nonconviction data* oder der Übermittlung von Strafregistrierungen an eine andere Behörde als Strafverfolgungsbehörden sind bestimmte Schranken erforderlich. Außerdem müssen bei Datenanfragen Protokolle angefertigt werden oder es muss für eine entsprechende Ausbildung des Personals gesorgt werden, das am Strafregistersystem beteiligt ist. Die Übermittlung der Strafregistrierungen an eine Behörde setzt

---

ber überprüfen kriminelle Hintergrunddaten aus offiziellen Quellen (Vgl. *Pager*, The Mark of a Criminal Record, S. 953).

618 Siehe *Mukherji*, In Search of Redemption: Expungement of Federal Criminal Records, S. 6.

619 *Jacobs/Crepet*, The Expanding Scope, Use and Availability of Criminal Records, Legislation and Public Policy, Vol 11, 2008, 177, 186 f. m. w. N.

620 42 U. S. C. § 14616 IV (c).

aber keine Möglichkeit der Betroffenen voraus, auf Verlangen Einsicht zu nehmen. Die Behörde ist auch nicht dazu verpflichtet, die Betroffenen darüber zu benachrichtigen. Bei der Verwendung des Strafregisters zur Strafrechtspflege scheint der Aspekt des Privacy-Schutzes, also des Datenschutzes, nicht genügend berücksichtigt zu werden. Die Verwendung ist ausschließlich mit gesetzlich vorgesehenen bestimmten Zwecken verbunden.

Die Politik konzentriert sich viel mehr auf die Versorgung mit genauen Daten als auf den Datenschutz. Dafür wurden einige gesetzliche Sicherungsvorkehrungen getroffen, damit sichergestellt wird, dass die staatlichen *criminal history records* vollständig, genau, für berechtigte Nutzer leicht zugänglich und vertrauensvoll sind. Zu diesen Vorkehrungen zählen u. a. die Mitteilungspflicht innerhalb von 90 Tagen nach den Verfügungen sowie der Prozess der systematischen Prüfung im Rahmen der Datenerhebung der -eintragung und der -speicherung.

d) Speicherdauer

Die bundesgesetzliche Regelung über die Speicherdauer von Daten im Strafregister existiert nur in Form von Ausnahmen. Die Datenspeicherung auf staatlicher Ebene ist jedem einzelnen Bundesstaat anvertraut. Die Strafregistrierungen werden in den meisten Fällen auf unbegrenzte Zeit bestehen.[621] Die Speicherdauer der Daten im Strafregister wird zwar einzelstaatlich auch nicht normiert, jeder einzelne Bundesstaat stellt jedoch die Begünstigungsmaßnahme der Tilgung[622] der Daten unter bestimmten Umständen[623] zur Verfügung. Die Voraussetzung zur Tilgung ist je nach Staat unterschiedlich. In einigen Staaten können nur die Verhaftungsdaten ohne Verurteilungen getilgt werden, in anderen auch die Verurteilungsdaten. Ob ein ehemaliger Straftäter die Tilgung seiner Strafregistrierung genießen kann, hängt davon ab, wo er angeklagt wurde. Aber es gibt Gemeinsamkeiten: Ein erstmaliges Vergehen insbesondere von einem Minderjährigen wird meist nach einer gewissen Zeit getilgt. In den meisten

621 *Jacobs*, Mass Incarceration and the Proliferation of Criminal Records, Vol. 3 Issue 3, Univ. Of St. Thomas Law Journal, S. 393.

622 Hierbei wird unter *Tilgung* die Rechtsfolge verstanden, nach der die behördlichen Daten der Öffentlichkeit nicht zugänglich gemacht werden. Zu Einzelheiten siehe auch oben Fn. 469.

623 Zum Beispiel innerhalb eines bestimmten Zeitraums, in der Regel mehr als ein Jahr (Vgl. *Jacobs*, Mass Incarceration and the Proliferation of Criminal Records, Vol. 3 Issue 3, Univ. Of St. Thomas Law Journal, S. 393 m. w. N.).

Einzelstaaten ist es unmöglich, die Strafregistrierungen wegen sexueller Verbrechen zu löschen. Den Verhaftungsdaten ohne Verurteilungen ist in 36 Einzelstaaten die Möglichkeit der Tilgung gegeben.

Auch wenn eine Löschung landesgesetzlich vorgesehen ist, erfolgt sie nicht automatisch. In der Regel muss sich die die Löschung ersuchende Person bei einer zuständigen Behörde bewerben und von sich aus Unterlagen dafür vorlegen. Im US-amerikanischen System, in dem Strafregistrierungen nicht nur in den staatlichen Strafregistern, sondern auch in den Datenbanken aller Gerichte und kommerzieller Informationsanbieter zur Verfügung gestellt werden, kann die Löschung von Daten nur im Strafregister ihre praktische Bedeutung verlieren und damit das einheitliche Datenmanagement unmöglich machen. Entsprechendes gilt für das Versiegeln von Daten im Strafregister. Darüber hinaus besteht hier sogar ein Risiko, die versiegelten Daten absichtlich oder versehentlich offenzulegen. Ein weiteres Problem liegt zudem in der Wirksamkeit der Versiegelung von Daten unter modernen automatisierten Bedingungen. Der Versiegelung oder Löschung kann kaum Bedeutung zukommen, wenn bestimmte Daten für eine bestimmte Zeit auf einer Webseite veröffentlicht werden können. Diese Probleme sind deshalb ernst, weil ein Verwertungsverbot nach einer Löschung oder Sperrung gesetzlich nicht vorgesehen ist.

3. Vergleich

a) Organisationsstruktur

Die Strafregistersysteme in Deutschland und den USA zeigen vor allem einen konstruktiven Unterschied. In Deutschland wird das BZR abgesehen vom ZStV als ein einheitliches Strafregister geführt, das umfassende und schnell verfügbare Informationen über einen Beschuldigten in einem Ermittlungsverfahren bis vor deren Eintragung ins BZR zur Verfügung stellt.[624] Demgegenüber wird in den USA ein zentrales Strafregister mit Verweis auf dessen mangelnde Effektivität absichtlich vermieden[625] und stattdessen auf ein dezentrales Strafregistersystem gesetzt, in dem die

624 BT-Drs. 12/6853, S. 3; *Gieg*, KK-StPO, § 494 Rn. 4.

625 *Jacobs/Blitsa*, Sharing Criminal Records: The United States, the European Union and Interpol Compared, 30 Loy. L.A. Int'l & Comp. L. Rev. 125 (2008) /Loyola of Los Angeles International and Comparative Law Review, Vol. 30, Issue 2 (Spring 2008), pp. 125–210 (130 f.).

jeweils von allen Bundesstaaten und dem FBI gesondert geführten Strafregister unter dem III-System (*Interstate Identification Index*) miteinander verbunden werden. In solchen dezentralen Strafregister werden alle strafrechtlich relevanten Daten, also nicht nur die Verurteilungsdaten, sondern auch die bloßen Verhaftungsdaten ohne Verurteilungen, gespeichert.

Unter der deutschen Strafprozessordnung flankieren einige gesetzliche Regelungen im Rahmen der Erhebung, der Speicherung, der Übermittlung und der Weitergabe von Daten das Strafregistersystem (BZR und ZStV), wodurch einem unbefugten oder übermäßigen Zugriff auf diese Daten vorgebeugt werden soll. Bei der Erhebung werden die mitteilungspflichtigen Stellen begrenzt und namentlich im Gesetz aufgeführt und die in das Register einzutragenden Inhalte, Erhebungs-, Anfrage- und Übermittlungsmethode und obligatorische Mitteilungsfristen sind ebenfalls konkret vorgesehen. Zur Speicherung im Strafregister müssen die Daten einige Prüfungen bestehen. Das Verfahren und die Methode der Übermittlung (die Auskunft auf Ersuchen) sind im Einzelnen beschrieben. Danach teilt eine mitteilungspflichtige Stelle der Registerbehörde die einzutragenden Inhalte innerhalb einer für die Daten bestimmten Mitteilungsfrist mittels Fernübertragung mit. Die Daten werden nach einigen Prüfungen für eventuelle Anfragen gespeichert. Eine berechtigte Stelle stellt nach festgelegten Verfahren eine Anfrage zu den in Gesetzen ermächtigten Zwecken. Die Registerbehörde prüft die Berechtigung der Stelle und des angegebenen Zweckes und erteilt dann der Stelle auf Anfrage eine Auskunft mittels Datenübertragung oder eines automatisierten Verfahrens (Abruf). Die Weitergabe der von der Registerbehörde erhaltenen Daten ist grundsätzlich verboten, aber ausnahmsweise zulässig, wenn dies zur Vermeidung von Nachteilen für den Bund oder ein Land unerlässlich ist oder wenn andernfalls die Erfüllung öffentlicher Aufgaben erheblich gefährdet oder erschwert würde. Die übermittelten Daten sind nach ihrer Verwendung unverzüglich zu löschen. Die Daten im Strafregister werden nicht dauerhaft gespeichert, sondern nach vorher festgelegten Fristen vollends gelöscht.

Das US-amerikanische Strafregistersystem geht einen völlig anderen Weg. Die Bundesgesetze, auf denen das III-System basiert, regeln nur den Austausch von Daten unter dem III-System und die Erhebungs- und Speicherregelung im staatlichen Strafregistersystem ist jedem einzelnen Bundesstaat überlassen. Die Erhebung, Speicherung, Übermittlung und Weitergabe von Daten auf staatlicher Ebene werden also je nach Bundesstaat unterschiedlich geregelt. Das III-System verbindet einen ersuchenden Staat nur mit dem Staat, der die ersuchten Daten in seinem Strafregister

erhält, aber beeinflusst nicht die Führung des staatlichen Strafregisters. Jeder Staat besitzt damit verschiedene Regelungen über die mitteilungspflichtigen Stellen, die Mitteilungsmethoden sowie -fristen und die einzutragenden Daten. Die Mitteilung der Strafregistrierungen an das III-System variiert außerdem in Abhängigkeit davon, ob die einzelnen Bundesstaaten am NFF teilnehmen oder nicht. Abgesehen von den unterschiedlichen Regelungen über das Strafregistersystem unter allen Staaten teilen die am NFF teilnehmenden Staaten dem FBI alle ersten Registrierungsdaten mit, die nicht daran teilnehmenden Staaten hingegen alle Strafregistrierungen. Mit diesen Daten gewinnen das NFF und der Index Aktualität. Die ersuchende Stelle stellt ihre Anfrage über ihr staatliches Strafregister an das FBI. Der III-Computer verweist das staatliche Strafregister an das FBI und/oder an ein oder mehrere der staatlichen Strafregister, die die angefragten Daten erhalten. Die angegebenen Quellen schicken die Antwort, die dann vom staatlichen Strafregister zur anfragenden Behörde weitergeleitet wird. Drei Arten von Computernetzwerken stehen in diesem Prozess für eine Anfrage und Antwort zur Verfügung. Die Übermittlung von *conviction data*, die Weitergabe oder die Vernichtung der übermittelten Daten und die Löschung von in staatlichen Strafregistern gespeicherten Daten werden bundesgesetzlich nicht geregelt.

b) Inhalt des Registers

Ein Unterschied beim Strafregistersystem in den beiden Ländern liegt im Inhalt des Registers. Während in Deutschland die Verurteilungsdaten und die Strafverfahrensdaten nach unterschiedlichen Regeln separat gespeichert und verarbeitet werden, werden in den USA die beiden Datenarten zusammen in Strafregister eingetragen und gespeichert. Die Strafverfahrensdaten im ZStV werden also entweder ins BZR eingetragen und dann gelöscht oder bei Nichteintragung nach einer gewissen Zeit vollständig gelöscht. Demgegenüber bleiben neben den Verurteilungsdaten die bloßen Verhaftungsdaten im Strafregister gespeichert, was für den Betroffenen dauerhaft nachteilig sein kann.[626]

626 Eine nachteilige Verfügung kann auch nur aus der Verhaftung vor einer Verurteilung begründet werden. Zu einer näheren Betrachtung der Nachteile siehe oben Teil 3 B. I. 4. und Department of Housing and Urban Development v. Rucker, 535 U. S. 125.

Während in Deutschland die sowohl im BZR als auch im ZStV einzutragenden Daten bundesgesetzlich geregelt werden, gibt es in den USA nichts Entsprechendes. Das BZRG und § 492 Abs. 2 StPO als die Rechtsgrundlage des ZStV sehen die ausführlichen Kataloge vor. Unter dem deutschen Strafregistersystem werden neben strafgerichtlichen Verurteilungen noch weitere Daten gespeichert; daher wurde das System in *Bundeszentralregister* umbenannt. Unter dem US-amerikanischen III-System, das dem Austausch von Strafregistrierungsdaten zwischen dem Bund und den Einzelstaaten dient, ist nur vorgesehen, dass die Mitteilung der Strafregistrierungen unbeschadet der unterschiedlichen Praxis des Strafregisters in jedem Staat nur für schwere und/oder erhebliche Erwachsenen- und Jugendstraftaten erfolgen darf.

c) Verwendung der Daten aus dem Register

Beim Datenschutz ist der Schutz vor der unbefugten oder übermäßigen Verwendung und Weitergabe personenbezogener Daten genauso bedeutsam wie der Schutz vor der unbegrenzten Erhebung und Speicherung personenbezogener Daten. Dieser Schutz setzt voraus, dass die Möglichkeit zur Korrektur von Fehlinformationen durch die Falschverarbeitung dem Einzelnen offenstehen muss und dass die Betroffenen nachvollziehen können, welche ihrer Daten von wem in welchem Verwendungszusammenhang weiterverarbeitet werden. Dafür sind die präzise Normklarheit, die Zweckbestimmung und -bindung sowie die Mitteilung an die Betroffenen erforderlich. Hierbei soll das Strafregistersystem in den beiden Ländern unter Maßgabe des Kriteriums betrachtet werden, welche Sicherheitsmaßnahmen verfügbar sind, um den Einzelnen gegen die mögliche missbräuchliche Verwendung seiner personenbezogenen Daten zu schützen. Denn beim Strafregistersystem kommt der Abwägung der unterschiedlichen Interessen eine wichtige Bedeutung zu: zum einen das Interesse der Verurteilten an einer Resozialisierung, insbesondere an der Erlangung einer neuen Arbeitsstelle und zum anderen das Interesse Dritter, insbesondere der Arbeitgeber an der Kenntnis belastender, für eine Einstellung maßgebender Gesichtspunkte und das öffentliche Interesses an einer brauchbaren Grundlage für Verwaltungsentscheidungen.[627]

Von Eintragungen im deutschen BZR darf grundsätzlich nur der Betroffene und unter bestimmten Voraussetzungen auch bestimmte Behörden

627 *Tolzmann*, Bundeszentralregistergesetz, § 30 Rn. 7.

Kenntnis nehmen. Die Auskunftsmöglichkeiten haben je nach Empfängerkreis unterschiedliche Inhalte. Die Staatsanwaltschaft und das Strafgericht erhalten in bestimmten Fällen eine weitergehende Auskunft als die übrigen Auskunftsberechtigten.[628] In das Führungszeugnis für private Zwecke wird hingegen nur ein begrenzter Ausschnitt der tatsächlich möglichen Eintragungen – nur die strafrechtlichen Verurteilungen (§ 4 BZRG) mit Ausnahmen von §§ 32 bis 34, 39 BZRG – aufgenommen. Dies ist das Ergebnis einer sorgfältigen Abwägung widersprüchlicher Interessen. Das zielt darauf ab, dass die Wiedereingliederung der Bestraften in Beruf und Gesellschaft dadurch erleichtert wird, dass bestimmte Bestrafungen überhaupt nicht, andere nach Ablauf bestimmter Fristen nicht mehr in das Privatführungszeugnis aufgenommen werden. Damit die Möglichkeit der Aushändigung des Zeugnisses an Unbefugte ausgeschlossen wird, darf das Führungszeugnis grundsätzlich nur an die Antragstellenden geschickt werden, und die Meldebehörde ist dazu verpflichtet, die Identität der Antragstellenden und die Angaben zum Wohnsitz zu überprüfen. Aus dem gleichen Grund ist die Übersendung der zur Vorlage bei einer Behörde bestimmten Zeugnisse, also der Behördenführungszeugnisse, an die Antragstellenden gesetzlich verboten. Denn in diese Zeugnisse werden auch Eintragungen aufgenommen, die im Privatführungszeugnis nicht erscheinen. Dadurch wird die missbräuchliche Verwendung personenbezogener Daten verhindert: Schutzvorschriften könnten ansonsten z. B. dadurch umgangen werden, dass die Arbeitgeber die Betroffenen dazu veranlassen, ein angeblich zur Vorlage bei einer Behörde bestimmtes Zeugnis zu beantragen und dann ihnen zu zeigen.[629] Außer wenn die Auskunft unmittelbar dem Betroffenen oder ggf. seinem gesetzlichen Vertreter erteilt wird, ist der Auskunftsantrag gesetzlich an bestimmte Voraussetzungen gebunden, damit die Betroffenen gegen die missbräuchliche Verwendung ihrer personenbezogenen Daten effektiv geschützt werden können. Dazu gehört das Verbot der Übersendung des Behördenführungszeugnisses an die Antragstellenden. Darüber hinaus wird vorausgesetzt, dass das Führungszeugnis zur Erledigung der hoheitlichen Aufgaben der Behörden benötigt wird und eine Aufforderung an den Betroffenen, ein Führungszeugnis vorzulegen, nicht sachgemäß oder erfolglos bleibt. Die Weitergabe des Behördenführungszeugnisses an eine andere Behörde ist nur unter der Einwilligung der Betroffenen möglich.

628 Für eine Übersicht über den inhaltlichen Unterschied je nach Empfängerkreis siehe *Tolzmann*, Bundeszentralregistergesetz, § 3 Rn. 18.

629 *Tolzmann*, Bundeszentralregistergesetz, § 30 Rn. 33.

Bei unbeschränkter Auskunft nach § 41 BZRG, mit der der gesamte Inhalt des Registers lediglich einer eng begrenzten Zahl von Behörden im überwiegend öffentlichen Interesse an dem Schutz vor der Begehung weiterer Straftaten zur Kenntnis gebracht wird, sind zur Gewährleistung des Schutzes dieser hochsensiblen Daten und zur Verhinderung ihrer missbräuchlichen Verwendung Schranken eingebaut worden: die abschließende Aufzählung der auskunftsberechtigten Stellen, die Begrenzung auf Einzelfallanfragen und die Beschränkung der Auskunftserteilung auf bestimmte Zwecke. Die unbeschränkt auskunftsberechtigte Stelle muss also den Zweck der Anfrage angeben und die Registerbehörde muss prüfen, ob der angegebene Zweck ein Recht auf unbeschränkte Auskunft gibt. Die Auskunft darf nur für diesen Zweck verwertet werden. Damit wird die Weitergabe unbeschränkter Auskünfte grundsätzlich mit der Ausnahme der Weiterleitungsmöglichkeit nach § 43 BZRG verboten. Die Ausnahme dient aber dazu, den Umfang der Verwendung der Daten, die die obersten Bundes- und Landesbehörden gem. § 41 Abs. 1 BZRG ohne konkrete Zweckbeschränkung erhalten, einzugrenzen. Die Weitergabe darf nur an die der obersten Behörde unterstellten Behörden erfolgen, wenn dies zur Vermeidung von Nachteilen für Bund oder Land unerlässlich ist, weil die Erfüllung öffentlicher Aufgaben andernfalls erheblich gefährdet oder erschwert würde.

Für die Strafverfahrensdaten von Beschuldigten und Tatbeteiligten sind nur die Strafverfolgungsbehörden auskunftsberechtigt. Sie dürfen diese Daten – mit einigen Ausnahmen – aber ausschließlich für Strafverfahren speichern, verändern und verwenden. Die Strafverfahrensdaten ohne Verurteilung werden im BZR gespeichert und zugleich aus dem ZStV gelöscht. Wird der Beschuldigte rechtskräftig freigesprochen, die Eröffnung des Hauptverfahrens gegen ihn unanfechtbar abgelehnt oder das Verfahren nicht nur vorläufig eingestellt, werden die Strafverfahrensdaten hingegen nach Ablauf einer bestimmten Zeit aus dem ZStV gelöscht und damit von niemandem verwendet. Da die Verwendung der Strafverfahrensdaten an den Verwendungszweck gebunden ist, dürfen die Daten nur zu dem Zweck verwendet werden, für den sie übermittelt wurden. Eine Verwendung für andere Zwecke wird nur insoweit erlaubt, als die Daten dafür hätten übermittelt werden dürfen.

Da die Verwendung personenbezogener Daten sowohl aus dem BZR als auch aus dem ZStV nicht mit der Verpflichtung verbunden ist, die Betroffenen darüber zu unterrichten, werden diese Daten normalerweise ohne das Wissen der Betroffenen verwendet, außer wenn die Betroffenen ein Führungszeugnis zur Vorlage bei einer Behörde beantragen. Statt der Un-

terrichtungspflicht sind jedoch die Verwendungsberechtigten, der Verwendungszweck und die Weitergabe schon übermittelter Daten gesetzlich eng eingeschränkt, um den Einzelnen gegen eine unbefugte oder unbegrenzte Verwendung personenbezogener Daten zu schützen. Die Betroffenen sind außerdem dazu berechtigt, die Eintragungen im BZR und im ZStV einzusehen. Das Einsichtsrecht dient dazu, die Wahrscheinlichkeit falscher Informationen zu verringern. Auf das Einsichtsrecht sind die Antragstellenden von der Meldebehörde hinzuweisen. Darüber hinaus werden die erforderlichen und angemessenen Maßnahmen gesetzlich gefordert, um die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit der im Register gespeicherten Daten entsprechend dem jeweiligen Stand der Technik sicherzustellen.

Rechtliche Vorkehrungen zum Schutz eines Einzelnen vor unbefugter oder unbegrenzter Verwendung von Eintragungen aus dem Strafregister sollen in den USA jeweils getrennt auf bundesstaatlicher Ebene und auf einzelstaatlicher Ebene berücksichtigt werden. Die bundesgesetzlichen Einschränkungen der Datenverwendung unter dem III-System und FIRS, das dem zwischenstaatlichen Datenaustausch dient, sind in 28 C. F. R. § 20.33 geregelt. Hierbei sind die Auskunftsberechtigten in Verbindung mit bestimmten Verwendungszwecken genannt. Ebenso wie in Deutschland sind in den USA die Verwendungsberechtigten und der Verwendungszweck von Strafregistrierungen auf bundesstaatlicher Ebene eingeschränkt. Die Strafgerichte und Strafverfolgungsbehörden dürfen z. B. auf die Strafregistrierungen, die im III-System und FIRS enthalten sind, für Zwecke der Strafrechtspflege oder der Durchführung von Hintergrundkontrollen im Rahmen des *national instant criminal background check system* (NICS) zugreifen. Die Strafregistrierungen dürfen an gesetzlich berechtigte Bundesbehörden oder zur Verwendung im Zusammenhang mit der Lizenzierung oder Beschäftigung übermittelt werden. Die Verwendung der auf diese Weise übermittelten Daten beschränkt sich zweckgebunden auf die genannten Behörden und damit ist die Weitergabe der Daten an eine andere Behörde grundsätzlich verboten (28 C. F. R. § 20.33 (b)). Außerdem können die Betroffenen ihre Daten vom FBI erhalten, um die Gefahr von Fehlinformation zu reduzieren. Der *Code of Federal Regulations* fordert, dass geeignete Maßnahmen getroffen werden, um die Vollständigkeit, Genauigkeit und Sicherheit von Strafregistrierungen zu gewährleisten.

Die Verwendung von Eintragungen auf einzelstaatlicher Ebene regelt zuerst bundesgesetzlich 28 C. F. R. § 20.21 (b) und (c). Die Vorschrift beschränkt nur die Verwendung von *nonconviction data*. Diese Daten

dürfen nur an Strafgerichte und Strafverfolgungsbehörden für Zwecke der Strafrechtspflege und an Einzelpersonen und Behörden für jeden Zweck, der durch Gesetze, Verordnungen, Verfügungen oder Gerichtsurteile, -entscheidungen oder -ordnungen genehmigt wurde, aufgrund einer spezifischen Vereinbarung mit einer Strafverfolgungsbehörde oder für den ausdrücklichen Zweck der Forschung, Evaluation oder Statistik im Rahmen einer Vereinbarung mit einer Strafverfolgungsbehörde übermittelt werden. Diese Regelung bestimmt außerdem, dass die Verwendung von Strafregistrierungen, die an eine andere als die justizielle Behörde übermittelt wurden, auf den Zweck beschränkt ist, für den sie erteilt wurden (Zweckbindung), und dass die Übermittlung von Daten über Verfahren in Bezug auf die Entscheidung eines Jugendlichen an eine andere als die justizielle Behörde verboten ist. Auf Grundlage dieses Bundesgesetzes regelt jeder Einzelstaat auf staatlicher Ebene abhängig von der Datenart – *conviction data*, *nonconviction data* und *arrest data* – unterschiedliche Einschränkungen.[630] Maryland kennt Ermächtigungsgrundlagen, auf denen jede Art von Daten jeweils an die justiziellen Behörden, die anderen Behörden oder zum privaten Sektor übermittelt werden darf. Dazu gehören Normen, die eine Hintergrundprüfung in bestimmten Bereichen erlauben oder sogar beauftragen. Während in Maryland kein Übermittlungsverbot dieser drei Datenarten vorgesehen ist, verbietet Kalifornien eine Datenübermittlung in bestimmten Bereichen.[631]

Werden die Gesetzgebungen über die Verwendung von Strafregistrierungen zusammengefasst, lässt sich Folgendes feststellen: Die Verwendung von *conviction data* ist im Bundesgesetz grundsätzlich unbeschränkt und jeder Staat verfügt demnach über Ermächtigungsnormen, die es ermöglichen, Daten an die strafjustiziellen sowie die anderen Behörden oder den privaten Sektor zu übermitteln. Die Übermittlung von *nonconviction data* an eine Strafjustizbehörde, die anderen Behörden oder den privaten Sektor ist bundesgesetzlich nur zu Strafverfolgungszwecken, zu gesetzlich berechtigten Zwecken oder aufgrund einer besonderen Vereinbarung mit einer Justizbehörde zulässig. In diesem Fall ist die Verwendung an einen genannten Zweck gebunden. Jeder Einzelstaat ermöglicht die Verwendung von *nonconviction data* und sogar *arrest data* mit entsprechenden Ermächtigungsgrundlagen. Dies führt schließlich zu der folgenden Bewertung:

630 Zu Einzelheiten der rechtlichen Grundlagen der einzelstaatlichen Datenübermittlung siehe *U. S. Department of Justice*, Compendium of State Privacy and Security Legislation: 2002 Overview, Bureau of Justice Statistics, 2003.

631 Labor Code 432.7.

Jede Art von Daten darf ohne Einschränkung verwendet werden, solange es eine entsprechende Ermächtigungsnorm gibt. Denn es gibt sowohl bundesgesetzlich als auch einzelstaatlich so gut wie keine Beschränkung der Verwendung von *conviction data*, *nonconviction data* oder *arrest data*. Außer der Einschränkung von Strafregistrierungen, die im Rahmen des III-Systems übermittelt werden dürfen, gibt es also keine besonderen Beschränkungen für die Verwendung von Strafregistrierung, um einen Einzelnen vor einer unbegrenzten Verwendung zu schützen.

Die bundes- und einzelstaatsgesetzlich erlaubten oder sogar beauftragten kriminalpolizeilichen Überprüfungen in bestimmten Bereichen, Megans Gesetze und die Zunahme der privaten Informationsdienstunternehmen führen dazu, dass jeder nur mit Namensangabe gegen eine Gebühr die *conviction data* oder sogar die *arrest data* von jemandem erhalten kann – obwohl die gesetzlichen Grundlagen in jedem Staat unterschiedlich sind.[632] Dafür gibt es nur eine Einschränkung, nämlich, dass die Daten nicht für den Zweck einer Beschäftigungsentscheidung verwendet werden dürfen.[633] Dies macht die Strafregistrierungen einer anderen Person zu niedrigen Kosten für jedermann leicht zugänglich. Eine Weitergabe der Daten an eine andere Behörde, die unter dem III-System, aufgrund einer Hintergrundprüfung oder von privaten Informationsdienstunternehmen erhalten wurden, ist weder verboten noch eingeschränkt.

Wie oben bereits erwähnt, wurden in Deutschland verschiedene Maßnahmen ergriffen, um eine unbefugte oder unbegrenzte Verwendung personenbezogener Daten in Bezug auf die Vorbestrafungen zu verhindern. Die Auskunftsberechtigten, die Verwendungszwecke, die aufzunehmenden Eintragungen nach Auskunftsweise und Weitergabe schon übermittelter Auskünfte sind unter der Abwägung des Interesses der Allgemeinheit an der Abwehr besonderer Gefahren und des Interesses des Betroffenen an einer möglichst reibungslosen Wiedereingliederung gesetzlich konkret geregelt. Obwohl die Strafregistrierungen in der Politik tendenziell allgemein zugänglicher werden, scheinen in den USA fast keine Einschränkungen zur Vermeidung einer unbegrenzten oder übermäßigen Nutzung von Strafregistrierungen vorgesehen zu sein, unabhängig davon, ob sie zu den

632 Private Informationsdienstunternehmen warnen Arbeitgeber, Vermieter, Hotels und andere Unternehmen davor, dass die unterlassenen Hintergrundprüfungen zu erheblicher Haftung wegen unerlaubter Handlungen führen könnten (*Jacobs/Crepet*, The Expanding Scope, Use and Availability of Criminal Records, Legislation and Public Policy, Vol 11, 2008, 177, 178).

633 *Jacobs/Crepet*, The Expanding Scope, Use and Availability of Criminal Records, Legislation and Public Policy, Vol 11, 2008, 177, 187 m. w. N.

conviction data oder *nonconviction data* gehören.[634] Die Politik scheint sich hier viel mehr auf die Versorgung mit genauen Daten als auf den Datenschutz zu konzentrieren. Denn ebenso wie Deutschland fordern die USA dazu auf, technische Maßnahmen zu treffen, um die Vollständigkeit, die Genauigkeit und die Sicherheit der Daten sicherzustellen. Gemeinsam ist die Gewährleistung des Einsichtsrechts der Betroffenen, um Fehlinformationen zu korrigieren. Anders als in Deutschland, wo die Verwendung des Inhalts des Registers von der verhängten Strafe abhängt, richtet sich die Verwendung von Strafregistrierungen in den USA nach einer begangenen oder verdächtigten Straftat; dies spiegelt die Sensibilität der Gesellschaft für bestimmte Verbrechen wider. Im Falle etwa von Sexualdelikten oder Straftaten im Zusammenhang mit häuslicher Gewalt werden nicht nur die *conviction data*, sondern auch die *arrest data* in den besonderen Registern gespeichert und zur Verfügung gestellt. Insbesondere für Sexualstraftäter stehen aufgrund der Verbreitung der Megans Gesetze und des *Adam Walsh*-Gesetzes erhebliche personenbezogene Daten aus dem Strafregister kostenlos online zur Verfügung.

d) Speicherdauer

Während das deutsche Strafregistersystem bundesgesetzlich einheitliche Vorschriften über die Speicherdauer von Daten sowohl im BZR und als auch im ZStV kennt, ist die Verarbeitung der Eintragungen in den einzelstaatlichen Strafregistern in den USA jedem Staat überlassen. Dies beruht auf dem Unterschied zwischen den politischen Strukturen der beiden Länder, obwohl beide Bundesstaaten sind. Bezüglich der Speicherdauer von Strafregistrierungen ist auf bundesstaatlicher Ebene – abgesehen von einigen Ausnahmen – keine einheitliche Vorschrift vorgesehen. Die meisten Einzelstaaten stellen in den USA zwar eine Form der Löschung von Strafregistrierungen oder ähnlichen Begünstigungen zur Verfügung. Aber die Voraussetzungen, die Mechanismen und die Objektverbrechen zur Tilgung unterscheiden sich voneinander. Ebenso wie bei der Speicherung strafrechtlich relevanter Daten erfolgt die Tilgung bestimmter Strafregistrierungen in einigen Staaten häufig, aber in anderen nicht. Ob die Strafregistrierung getilgt werden kann, hängt vom Anklage- und Ver-

634 *Jacobs*, Mass Incarceration and the Proliferation of Criminal Records, Vol. 3 Issue 3, Univ. Of St. Thomas Law Journal, S. 419.

handlungsort ab.[635] Aber die Verurteilungsdaten werden normalerweise nicht getilgt, auch wenn sie in wenigen Staaten unter bestimmten Voraussetzungen gelöscht werden können. Dies gilt insbesondere im Falle von Verurteilungsdaten wegen sexueller Verbrechen. Daraus ergibt sich, dass das öffentliche Interesse daran, die Strafregistrierungen für zukünftige Verbrechensermittlungen beizubehalten, dem individuellen Interesse des Betroffenen an seinen Verurteilungsdaten überlegen ist. Außerdem werden die Strafregistrierungen in einigen Staaten dann automatisch getilgt, wenn bestimmte Voraussetzungen erfüllt sind, aber in anderen muss eine auf eine Tilgung ersuchende Person die tatsächliche Unschuld beweisen.[636] Das entscheidende Element bei der Tilgung ist nicht die Höhe der Hauptstrafe, sondern die Art des Verbrechens. Ein Beispiel bildet das sexuelle Verbrechen. Die Strafregistrierungen wegen sexueller Verbrechen werden aufgrund ihres höheren Rückfallrisikos schwer oder gar nicht getilgt.[637]

In Deutschland sind hingegen die Möglichkeiten der grundsätzlichen fristabhängigen Tilgung einerseits und der fristunabhängigen außergewöhnlichen Tilgung andererseits sowie der Sperrung als Ausnahmefall gesetzlich einheitlich vorgeschrieben. Eintragungen, die nach dem BZRG gespeichert werden, werden nach Ablauf einer bestimmten Frist grundsätzlich aus dem Register entfernt. Dabei richtet sich die Speicherdauer nach dem verhängten Strafmaß. Die Fristen werden bereits bei der Einordnung von Entscheidungen in das Register von einem Fristenprogramm berechnet und die zu tilgenden Daten werden bei der täglichen Überprüfung der Tilgungsfristen von einem besonderen Löschprogramm automatisch gelöscht.[638] Der Ablauf der Tilgungsfrist einer Verurteilung kann durch die in § 47 BZRG vorgesehene Voraussetzung gehemmt werden. Außerdem sind die fristunabhängige Entfernung von Entscheidungen aus dem Register gemäß §§ 16 Abs. 2, 24 und 63 BZRG und die vorzeitige Tilgung aufgrund einer Anordnung der Registerbehörde auf Antrag oder von Amts wegen möglich.

---

635 *Mukherji*, In Search of Redemption: Expungement of Federal Criminal Records, S. 8.

636 *Diehm*, Federal Expungement: A Concept in Need of a Definition, Federal Expungement: A Concept in Need of a Definition, St. John's Law Review, Vol 66. No. 1, 1992, 73, 74.

637 *McAdoo*, Creating an Expungement Statute for the District of Columbia: a Report and Proposed Legislation, S. 8.

638 *Rebmann*, Einhundert Jahre Strafregisterwesen in Deutschland, NJW 1983, 1513, 1516 f.

Der Tilgung kommt in Deutschland über die Bedeutung eines bloßen fristbezogenen Datenschutzes hinaus vor allem eine praktische Bedeutung zu. Eine Eintragung darf nach der Tilgung in den anderen späteren Strafverfahren nicht weiter verwertet werden (Verwertungsverbot). Hierbei steht dem Betroffenen das Schweigerecht zu. Demgegenüber ist die Begünstigungsmaßnahme der Tilgung in den USA nicht mit dem Verwertungsverbot verbunden. Denn das Wesen der Tilgung liegt nicht darin, die Daten tatsächlich zu löschen, sondern darin, die Daten für die Öffentlichkeit unzugänglich zu machen, und ein Mindestmaß an Daten wird damit typischerweise zur Aufbewahrung und zur weiteren Verwertung durch das Strafjustizsystem gesichert.

Abgesehen davon, dass es in den USA keine bundesgesetzliche Speicherdauervorschrift gibt und dass das Tilgungsregime je nach Einzelstaat unterschiedlich ist, liegt ein bedeutsamer Unterschied in der Behandlung der bloßen Strafverfahrensdaten. Wie oben bereits erwähnt, werden in den USA im Gegensatz zu Deutschland die Verhaftungsdaten ohne Verurteilungen auch im Strafregister gespeichert und können damit nachteilige Folgen für den Betroffenen haben. In einigen Staaten ist es sogar unmöglich, die Verhaftungsdaten zu tilgen, obwohl die Tatsache, dass eine Person schon einmal verhaftet, aber nicht verurteilt wurde, an nachteilige Verfügungen in vielen Bereichen geknüpft werden kann. Dementsprechend sind selbst zu Unrecht beschuldigte Personen von den Vorwürfen und dem damit verbundenen Stigma betroffen.

Die Verwendung der Eintragungen im deutschen ZStV wird hingegen durch zwei Möglichkeiten eingeschränkt: zum einen durch die Löschung, zum anderen durch die Sperrung. Die Speicherung im ZStV endet notwendigerweise, sobald die im ZStV gespeicherten Daten in das BZR eingetragen werden. Die Löschung beim ZStV erfolgt automatisch ebenso wie beim BZR, wenn die Löschungsvoraussetzung erfüllt wird. Die schon im ZStV gespeicherten, aber aufgrund des rechtskräftigen Freispruchs, der unanfechtbaren Ablehnung der Eröffnung des Hauptverfahrens und nicht nur vorläufiger sowie endgültiger Verfahrenseinstellung in das BZR nicht einzutragenden Daten werden erst zwei Jahre nach Verfahrenserledigung aus dem ZStV entfernt. Ein möglicher Nachteil aufgrund bloßer Strafverfahrensdaten wird damit abgesichert. Die schon entfernten Strafverfahrensdaten existieren entsprechend der Bedeutung des Wortes „Entfernung“ nicht mehr und können deshalb nicht weiter verwertet werden. Außerdem sind alle übermittelten Daten im Rahmen des ZStV nach ihrer Verwendung unverzüglich zu löschen. Neben der endgültigen Entfernung können die im ZStV gespeicherten Daten unter bestimmten Voraussetzun-

gen gesperrt werden. Die Verwendung der gesperrten Daten ist unter den im Gesetz vorgesehenen engen Ausnahmen verboten.

II. Rasterfahndung

1. Deutschland

a) Organisationsstruktur

Da im deutschen Datenschutzsystem jede Datenverarbeitung grundsätzlich verboten ist, ermächtigt die StPO mit § 98 a bis c die Strafverfolgungsbehörden dazu, die Daten automatisiert abzugleichen. Die Befugnis erstreckt sich dabei darauf, sowohl polizeiinterne als auch -externe Dateien, also Dateien, die bei einer öffentlichen Behörde oder einer privaten Stelle gespeichert sind, miteinander abzugleichen. Eine Rasterfahndung im eigentlichen Sinne (§ 98a StPO) beschränkt sich auf einen maschinell-automatisierten Datenabgleich zwischen bestimmten, auf den Täter vermutlich zutreffenden Prüfungsmerkmalen mit aus anderen Gründen an anderen Stellen gespeicherten Daten. Von der Rasterfahndung unterscheidet sich damit der Abgleich mit polizeiinternen Daten (z. B. der Abgleich personenbezogener Daten, die die Strafverfolgungsbehörden durch die in der StPO geregelten Ermittlungsmaßnahmen gewonnen haben, oder der Abgleich solcher Daten mit präventiv-polizeilichen Fahndungsdateien) in § 98c StPO. Auf Grundlage dieser Befugnis dürfen die Strafverfolgungsbehörden die Übermittlung der abzugleichenden Dateien von der Speicherstelle anfordern und die Speicherstelle soll dann die Daten aussondern und übermitteln und dabei die Strafverfolgungsbehörden unterstützen.

§ 98a Abs. 1 S. 1 StPO unterscheidet zwischen dem Ausschluss Nichtverdächtiger (negative Rasterfahndung) und der Feststellung von Personen, die weitere für die Ermittlungen bedeutsame Prüfungsmerkmale erfüllen (positive Rasterfahndung). Die beiden Arten der Fahndung unterscheiden sich in der Eingriffsintensität. Bei der positiven Rasterfahndung werden sämtliche Daten, die bei verschiedenen Behörden und privaten Einrichtungen gespeichert sind, durchsucht. Nicht nur die Daten, die letztlich auf dem Ergebnisband abgespeichert werden, sondern auch sämtliche Daten bei Suchläufen erfahren hier eine Änderung von ihrem ursprünglichen Bezugsrahmen in den Kontext polizeilicher Fahndungszwecke oder der Verdachtsüberprüfung. Daraus ergibt sich die Gefahr, dass die Personendaten ohne Kontrolle des Betroffenen zu einem teilweisen oder weitgehend voll-

ständigen Persönlichkeitsbild zusammengefügt werden. Damit sind sämtliche Personen, deren Daten sich in den zu untersuchenden Datenbeständen befinden, potenziell von weiteren Fahndungsmaßnahmen bedroht. Dies fördert die Tendenz zu möglichst unauffällig-konformem Verhalten und ist damit geeignet, die Wahrnehmung der allgemeinen Freiheitsrechte durch an Straftaten völlig Unbeteiligte einzuschränken.[639] Bei der negativen Rasterfahndung werden die Abgleichdateien nur dazu genutzt, Daten aus dem Ausgangsdatenbestand zu löschen. Die Abgleichdateien werden von den Strafverfolgungsbehörden nicht eingesehen und die betroffenen Dateninhaber werden von vornherein von Fahndungsmaßnahmen ausgeschlossen und sind somit nicht davon bedroht. Es verbleibt jedoch eine Missbrauchsgefahr, die einen psychischen Druck auf die Dateninhaber auslösen kann, vor dem das Recht auf informationelle Selbstbestimmung sie schützen soll. Bei der negativen Rasterfahndung mit einer Fremddatei als Ausgangsdatei wird die Ausgangsdatei von ihrem ursprünglichen Kontext in den polizeilichen Fahndungskontext überführt, während bei der negativen Rasterfahndung mit einer Ausgangsdatei, die zu Strafverfolgungszwecken angelegt ist, die Ausgangsdatei keine Zweckänderung erfährt.

b) Vergleichbare Daten

Die Rasterfahndung unterliegt hinsichtlich der personenbezogenen Daten, die für einen Datenabgleich verwendet werden dürfen, keinen Beschränkungen. Hinsichtlich Art, Inhalt und Umfang der zu Rasterfahndungszwecken heranzuziehenden Daten sieht die StPO keine nähere Erläuterung vor. Die fehlende Eingrenzung personenbezogener Daten kann die Gefahr dafür erhöhen, dass ein Persönlichkeitsprofil zustande kommt. Angesichts dieser Gefahr wurde im Zuge von Gesetzesentwürfen zwar eine Eingrenzung vorgeschlagen, diese Vorschlag hatte jedoch keinen Erfolg.

c) Verwendung des Datenabgleichs

Der Abgleich polizeiexterner Dateien ist gesetzlich mit bestimmten Voraussetzungen verbunden: den zureichenden tatsächlichen Anhaltspunkten

639 *Siebrecht*, Rasterfahndung – eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, S. 52.

hinsichtlich einer Katalogtat, die von erheblicher Bedeutung sein muss, der Subsidiarität der Maßnahmen und dem Richtervorbehalt. Nach § 98a Abs. 1 Satz 1 StPO ist eine Rasterfahndung also nur insoweit zulässig, als zureichende tatsächliche Anhaltspunkte dafür vorliegen, dass eine Katalogtat begangen wurde und wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise erheblich weniger erfolgversprechend oder wesentlich erschwert wäre. Die Übermittlung und der Abgleich polizeiexterner Daten dürfen nur auf der Grundlage einer gerichtlichen Anordnung oder bei Gefahr im Verzug auch aufgrund einer staatsanwaltschaftlichen Anordnung erfolgen.

d) Aufbewahrungsdauer der Daten

§ 98b Abs. 3 regelt die Rückgabe- oder die Löschungspflicht übermittelter Daten nach einem Datenabgleich. Danach sind die Daten auf Datenträgern nach Beendigung des Abgleichs unverzüglich zurückzugeben und personenbezogene Daten, die auf andere Datenträger übertragen wurden, sind unverzüglich zu löschen, sobald sie für das Strafverfahren nicht mehr benötigt werden. Es gibt aber keine Löschungs- oder Vernichtungsvorschrift für Daten, die aufgrund der staatsanwaltschaftlichen Eilanordnung erlangt wurden, jedoch gerichtlich nicht bestätigt wurden und damit außer Kraft treten.

e) Mitteilungspflicht

Zu benachrichtigen sind nach § 101 StPO von allen Betroffenen nur diejenigen, gegen die nach Auswertung der Daten weitere Ermittlungen geführt wurden. Somit fallen alle übrigen Betroffenen, deren personenbezogene Daten ebenfalls in die Rasterfahndung einbezogen waren, aus der Benachrichtigungspflicht heraus.[640] Die Benachrichtigung kann gesetzlich unterbleiben oder zurückgestellt werden. Wie oben bereits erwähnt, werden Personen, die von den Informationsverarbeitungsvorgängen im Zuge einer Rasterfahndung betroffen sind, in ihrem Recht auf informationelle Selbstbestimmung unterschiedlich intensiv beeinträchtigt. Diejenigen, die

640 *Siebrecht*, Rasterfahndung – eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, S. 140.

nach mehreren Suchläufen als Merkmalsträger herausgerastert wurden, sind intensiver betroffen als diejenigen, deren Daten sich nur in Abgleichdateien befinden, damit Personendaten aus dem Ausgangsdatenbestand gelöscht werden können. Trotzdem nimmt die StPO keinen Unterschied zwischen den beiden Fällen wahr, sondern schließt die Benachrichtigungspflicht mit weiteren Ermittlungen an. Das bedeutet, dass die Benachrichtigungspflicht letztlich nicht durch die Rasterfahndung an sich ausgelöst wird, sondern erst durch die dadurch veranlasste Vornahme weiterer Ermittlungen gegen diese Personen. Lediglich die Rasterfahndung löst also keine Benachrichtigungspflicht aus.

Über die Benachrichtigung der Betroffenen hinaus ist nach Beendigung einer Rasterfahndung die Stelle zu unterrichten, die für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz bei öffentlichen Stellen zuständig ist (§ 98b Abs. 4 StPO).

2. USA

a) Organisationsstruktur

Das *Computer Matching* ist ein computergestützter Abgleich von Datensätzen, der vornehmlich eingesetzt wird, um Gesetzesverstöße im Zusammenhang mit dem Empfang staatlicher Leistungen zu ermitteln. Durch US-amerikanische Gesetze wird nur der staatliche Datenabgleich geregelt, der die behördenübergreifende Datenübermittlung voraussetzt. Denn jede Datenverarbeitung ist in den USA grundsätzlich zulässig, soweit es keine spezielle Bestimmung gibt. Dies wird vor allem durch den Privacy Act und den Computer Matching Act als dessen Änderungsgesetz geregelt. Den besonders hohen Gefahren staatlicher automatisierter Datenverarbeitung wurde aber durch eine Einschränkung der behördenübergreifenden Übermittlung bei öffentlichen Stellen gespeicherter Daten Rechnung getragen (Privacy Act § 552a). Das Gesetz sieht insoweit ein Verbot der behördenübergreifenden Offenlegung personenbezogener Daten ohne Zustimmung der Betroffenen vor. Außerdem sind im Gesetz explizitere Richtlinien enthalten, die die Austauschmethode der Daten zwischen Behörden und das Ausmaß bestimmen, in dem die Behörden aufgrund von abgeglichenen Daten handeln dürfen. Eine behördenübergreifende Datenübermittlung darf nur auf Basis einer schriftlichen Vereinbarung zwischen einer Speicherstelle und einer Anfragestelle erfolgen, außer wenn ein *matching* im Anschluss an die Einleitung einer bestimmten strafrechtlichen oder zivil-

rechtlichen Untersuchung gegen eine oder mehrere bekannte Personen von einer Behörde durchgeführt wird, die jegliche Tätigkeit im Zusammenhang mit der Durchsetzung des Strafgesetzes als ihre Hauptaufgabe leistet, um Beweise gegen diese Person oder Personen zu sammeln.

Die Einschränkung erstreckt sich jedoch nicht auf die Übermittlungs- und Verarbeitungsvorgänge der Daten, über die eine Privatperson verfügt. Die Strafverfolgungsbehörden können den Zugang zu Daten im Privatbesitz durch einen entgeltlichen Erwerb beim Datenmarkt oder durch ein unmittelbares Ersuchen an den Privaten haben. Es gibt keine Regelung, nach der die Datenübermittlung Privater an die Strafverfolgungsbehörden verhindert oder aber zur Pflicht gemacht wird. Die Strafverfolgungsbehörden können Daten von Privatpersonen erhalten, aber nur, wenn diese dazu bereit sind. Viele Datenbesitzer willigen ohne eine *subpoena* oder eine gerichtliche Anordnung aber nicht ein, ihre Daten preiszugeben. Zum Zweck des Datenabgleichs dürfen die Strafverfolgungsbehörden somit die Datenübermittlung von einer anderen Behörde mit Zustimmung des Betroffenen fordern, personenbezogene Daten im Datenmarkt entgeltlich erwerben oder die Übermittlung privater Daten durch eine gerichtliche Anordnung erzwingen.

Die auf diese Weise erhaltenen Daten werden durch eine Reihe von Verfahren abgeglichen: einer Auswahl von Daten, einer Datenbereinigung, einem *matching*, einer Inferenz, einem Filtern der Treffer und einer Entscheidung aufgrund von Ergebnissen des Datenabgleichs.

b) Vergleichbare Daten

Beim Blick auf 5 U. S. C. § 552a (a) (4) kann festgestellt werden, dass die Vorschrift keine Beschränkung bezüglich Art, Inhalt und Umfang personenbezogener Daten vorsieht, die behördenübergreifend übermittelt und abgeglichen werden dürfen. Vergleichbare Daten nach dem 5 U. S. C. § 552a (a) (4) sind weder auf unsensible personenbezogene Daten noch auf Namen, Anschrift und Geburtsdatum der betreffenden Personen eingeschränkt. Sämtliche personenbezogenen Daten, die bereits bei einer Behörde gespeichert sind, können zum Zweck des Datenabgleichs herangezogen werden. Eine Behörde kann personenbezogene Daten erheben und speichern, indem sie die Daten durch Beobachtung der betroffenen Person oder ihres Verhaltens und als Nebenprodukt einer Transaktion zwischen der Behörde und der betroffenen Person erstellt sowie von der betroffenen Person selbst, von einer anderen Behörde oder von privaten

Datenbesitzern erwirbt. Die auf diese Weise erhobenen und dann gespeicherten Daten dürfen zum Gegenstand eines Datenabgleichs gemacht werden.

c) Verwendung des Datenabgleichs

Ein *Computer Matching* wird vor allem dazu durchgeführt, um die Berechtigung oder die fortwährende Einhaltung gesetzlicher und aufsichtsrechtlicher Anforderungen von Bewerbern, Empfängern oder Begünstigten von oder Teilnehmern an der Erbringung von Dienstleistungen in Bezug auf Geld- oder Sachleistungen oder Zahlungen im Rahmen von Bundesleistungsprogrammen festzustellen oder zu überprüfen, um Zahlungen zurückzuzahlen oder Schulden im Rahmen solcher Bundesleistungsprogramme zu tilgen.

Bei einer behördenübergreifenden Datenübermittlung zum Zweck eines Datenabgleichs bedarf es einer Zustimmung des Betroffenen, wenn es sich nicht um Fälle nach 5 U.S.C. 552a (b) (1) bis (12) handelt. Denn bei dieser Datenübermittlung müssen Daten eine Zweckentfremdung erfahren. Dies darf nur auf Basis einer Zustimmung der betroffenen Personen erfolgen. Diese Anforderung umgehen die Behörden häufig, indem sie den Ausnahmetatbestand in der Praxis großzügig auslegen und dann viele Abgleichvorgänge im Rahmen des Ausnahmetatbestandes durchführen oder indem sie behaupten, dass alle Datenübertragungen zwischen Regierungsstellen interne und nicht externe Übertragungen sind, weil sie angeblich Mitglieder eines monolithischen öffentlichen Dienstes sind. Diese Haltung kann es in der Praxis weniger sinnvoll oder sogar unmöglich machen, das Recht auf informationelle Selbstbestimmung durch spezifische Kontrollen mit verfahrensrechtlichen und organisatorischen Vorkehrungen zu schützen.

Eine behördenübergreifende Datenübermittlung zum Zweck eines Datenabgleichs darf nur auf Basis einer schriftlichen Vereinbarung zwischen einer Speicher- und einer Anfragestelle erfolgen. Die schriftliche Vereinbarung muss den Zweck des geplanten Datenabgleichs festlegen, die Datensätze beschreiben, abgeglichen werden, und das Verfahren zur Benachrichtigung über unerwünschte Ereignisse auf der Grundlage eines Datenabgleichs festlegen.

d) Aufbewahrungsdauer der Daten

Die Festlegung des Verfahrens zur Aufbewahrung und rechtzeitigen Vernichtung von Daten, die von einer Anfragestelle in einem Datenabgleich erstellt wurden, bleibt den Behörden zur Entscheidung überlassen. Das Verfahren hängt nur von der schriftlichen Vereinbarung ab. Geregelt ist nur, dass die Behörden Verfahren für die Rückgabe der Datensätze an die Speicherstelle oder die Vernichtung von Datensätzen erhalten müssen, die in einem Datenabgleich verwendet werden. Aber die Regelung gilt nur für den Abgleich, der die bei Behörden gespeicherten Daten verwendet. Bei privaten Daten wird diese Anforderung nicht angewendet. Es gibt hier keine Bestimmung über Aufbewahrungsfristen, Rückgabezeiten von Daten an eine Speicherstelle oder Löschungs- oder Vernichtungszeiten nach der Beendigung eines Abgleichs außer unter besonderen Umständen.

e) Mitteilungspflicht

Zum Schutz der Freiheitsrechte der Bürger sind neben den *vor* dem Abgleich erforderlichen Verfahren auch wichtige verfahrensrechtliche Vorkehrungen *nach* dem Datenabgleich getroffen. Die erste Maßnahme stellt die Forderung nach einer unabhängigen Überprüfung der Daten durch die Behörden dar, die an einem Datenabgleich teilgenommen haben. Keine nachteilige Entscheidung aufgrund von Ergebnissen eines Datenabgleichs darf außerdem getroffen werden, bis die Betroffenen über die mögliche Entscheidung benachrichtigt werden. Der Computer Matching Act verpflichtet die Behörden dazu, die Benachrichtigungsmethode der betroffenen Personen in der Vereinbarung anzugeben. Die Benachrichtigungspflicht wird hier nicht durch einen Datenabgleich, sondern durch nachteilige Maßnahmen aufgrund von Ergebnissen eines Datenabgleichs ausgelöst.

Die spezifische Kontrolle zum Schutz der Freiheitsrechte eines Einzelnen bilden die Auskunft des Kongresses sowie die Einrichtung eines Datenaufsichtsausschusses mit Berichtspflicht. Eine Kopie der schriftlichen Vereinbarung ist dreißig Tage vor Beginn der Maßnahme an einen Ausschuss des Kongresses zu schicken. Damit wird die parlamentarische Kontrolle der Maßnahme gesichert. Darüber hinaus müssen alle am *Computer Matching* beteiligten Behörden einen Datenaufsichtsausschuss einrichten. Er dient als ein behördeninternes Kontrollzentrum dazu, die Beachtung der Datenschutzvorschriften durch die Behörde zu überwachen und zu

koordinieren. Er soll einen jährlichen Bericht erstellen und diesen dem Leiter der Behörde und dem *Office of Management and Budget* vorlegen.

3. Vergleich

a) Organisationsstruktur

In Deutschland ist ein maschineller Datenabgleich grundsätzlich verboten und wird erst durch § 98a StPO erlaubt. In § 98a und 98b werden der mögliche Zweck und die Voraussetzungen eines Datenabgleichs, die Übermittlungs- und Unterstützungspflicht einer Speicherstelle, der Richtervorbehalt, eine Rückgabe bzw. Löschung schon ausgeglichener Daten, die Benachrichtigungspflicht der Betroffenen und die Unterrichtungspflicht der für die Kontrolle der Einhaltung der Vorschriften über den Datenschutz zuständigen Stelle konkret geregelt. In den USA ist eine Datenverarbeitung hingegen grundsätzlich erlaubt, soweit keine weiteren Bestimmungen gelten. Ein maschineller Datenabgleich wird also nur in den öffentlichen Bereichen eingeschränkt, aber nicht in den privaten. Denn der Computer Matching and Privacy Protection Act von 1988 legt nur die Verfahren für den Datenabgleich durch die Bundesbehörden fest.

Die deutsche Rasterfahndung ist gemäß § 98a StPO ein maschineller Abgleich von Daten, die sowohl bei öffentlichen als auch bei privaten Stellen bereits gespeichert sind, um Unverdächtige auszuschließen (negative Rasterfahndung) oder bestimmte Verdächtige festzustellen (positive Rasterfahndung). Nicht nur ermächtigt die Vorschrift die Strafverfolgungsbehörden dazu, an eine Speicherstelle das Ersuchen bezüglich bestimmter Daten zu richten und die Daten automatisch abzugleichen, sondern sie verpflichtet die Speicherstelle auch dazu, die Strafverfolgungsbehörden bei einem Datenabgleich zu unterstützen. Die Strafverfolgungsbehörden dürfen Daten einer anderen Stelle nur aufgrund dieser Bestimmungen anfordern und abgleichen. In den USA, wo jede Datenverarbeitung grundsätzlich zulässig ist, unterliegen demgegenüber angesichts hoher Gefahren bei der Datenverarbeitung durch den Staat nur solche Datenabgleiche Gesetzen, bei denen es einer behördenübergreifenden Datenübermittlung bedarf. Ein solcher Datenabgleich, also das *Computer Matching*, ist ein maschineller Abgleich von Daten, die nur bei öffentlichen Stellen bereits gespeichert sind, damit Verstöße vor allem in der Regierungsverwaltung, also im Hinblick auf staatliche Leistungsprogramme festgestellt werden. Es existiert keine spezifische Bestimmung, die von einer privaten Stelle eine

Übermittlung ihrer Datenbestände erzwingen kann, sondern die Strafverfolgungsbehörden können die Daten entweder entgeltlich am Datenmarkt kaufen oder direkt bei der privaten Stelle abhängig von ihrer Übermittlungsbereitschaft oder aufgrund einer gerichtlichen Übermittlungsanordnung erwerben.

Die Rasterfahndung und das *Computer Matching* beziehen die Vielzahl von Nichtverdächtigen ohne ein Vorliegen eines konkreten Verdachts ein. Die beiden Maßnahmen gehen von einem nichtindividualisierten Verdacht aus. Zur Anwendung der deutschen Rasterfahndung reichen zureichende tatsächliche Anhaltspunkte aus. Selbst der nach der Rasterung verbleibende „Bodensatz" weist noch keinen konkreten Tatenbezug auf, sondern dient als Ansatzpunkt für die konventionelle Fahndung, in deren Verlauf sich möglicherweise ein solcher Bezug herausstellt.[641] Es muss ohne einen täterbezogenen Verdacht lediglich der Verdacht vorliegen, dass eine bestimmte Straftat begangen wurde. Der Computer Matching Act setzt als eine Blankettnorm[642] zur Durchführung eines *Computer Matching* nicht einmal einen Anfangsverdacht voraus. Die Rasterfahndung dient als Mittel zur Einleitung konventioneller Ermittlungen, während das *Computer Matching* als eine Entscheidungshilfe funktioniert.

b) Vergleichbare Daten

Die Gemeinsamkeit zwischen den beiden Ländern liegt darin, dass bei den Daten, die für einen Datenabgleich zur Verfügung stehen, weder eine Einschränkung auf Namen, Anschrift und Geburtsdatum der betreffenden Personen noch eine Differenzierung zwischen sensiblen und unsensiblen Daten vorgesehen ist. Die deutsche Strafprozessordnung enthält keine nähere Erläuterung im Hinblick auf Art, Inhalt und Umfang der zu Rasterfahndungszwecken heranzuziehenden Daten. Die US-amerikanische Rechtsordnung zählt zwar konkrete für einen Abgleich verfügbare Daten auf, macht jedoch durch die Anwendung des Ausdrucks „nicht darauf beschränkt" das Nicht-Vorliegen einer Einschränkung deutlich. Solange Daten bereits bei einer anderen Stelle gespeichert sind und erhalten

641 *Siebrecht*, Rasterfahndung – eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung, S. 72.

642 *Gropp*, Rechtsvergleicher Querschnitt, in: Besondere Ermittlungsmaßnahmen zur Bekämpfung der Organisierten Kriminalität, 1993, 815 (844 f.).

werden können, dürfen alle personenbezogenen Daten unbegrenzt zum Datenabgleich herangezogen werden.

c) Verwendung des Datenabgleichs

Die deutsche Rasterfahndung ist mit bestimmten Voraussetzungen verbunden. Für die Zweckentfremdungsnutzung von Daten, also dafür, dass Daten, die für einen bestimmten Zweck erhoben wurden, später aber für einen anderen Zweck verwendet werden, sind einige verfahrensrechtliche Vorkehrungen in den beiden Ländern getroffen worden.

Als erste Voraussetzung fordert die Rasterfahndung ein Vorliegen zureichender tatsächlicher Anhaltspunkte dafür, dass eine Katalogtat von erheblicher Bedeutung, die in § 98a Abs. 1 Satz 1 aufgeführt wird, begangen wurde. Schwierigkeiten bezüglich des Begriffs „von erheblicher Bedeutung" und unüberschaubare Katalogtaten wurden schon oben erwähnt. Die zweite Voraussetzung ist die Subsidiarität der Rasterfahndung gegenüber konkurrierenden Maßnahmen. Eine Rasterfahndung darf nur dann angeordnet werden, wenn die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Täters auf andere Weise weniger erfolgversprechend oder wesentlich erschwert wäre. Drittens darf eine Rasterfahndung grundsätzlich durch einen Richter angeordnet werden. Damit wird den Gefahren einer Rasterfahndung begegnet. Der Richtervorbehalt kann aber durch die Möglichkeit der staatsanwaltschaftlichen Eilanordnung gefährdet werden, auch wenn diese nachträglich eine richterliche Entscheidung einholen muss. Angesichts der Bedeutung der Rasterfahndung ist es schwierig, die Umstände vorzustellen, unter denen eine staatsanwaltschaftliche Eilanordnung benötigt wird.

Der Computer Matching Act schließt eine Datenübermittlung zum Zweck eines Datenabgleichs an bestimmten Voraussetzungen an. Erstens ist eine Zustimmung der betroffenen Personen erforderlich. Eine Datenübermittlung ohne Zustimmung der Betroffenen ist grundsätzlich verboten. Aber die Anforderung wird in der Praxis durch die behördlichen totalitären Tendenzen und die weite Auslegung eines Ausnahmetatbestandes namens ‚routine use' vielfach umgangen. Dies schwächt die Bedeutung der Zustimmung des Betroffenen als eine Schwelle für die Datenübermittlung. Zweitens beinhaltet der Computer Matching Act keine inhaltlichen Leitlinien, sondern fordert für Datenübermittlungen zum Zweck eines Datenabgleichs, dass eine schriftliche Vereinbarung zwischen einer Speicherstelle und einer Anfragestelle getroffen wird. Die konkreten Inhalte

über die Vereinbarung werden nicht gesetzlich geregelt. Sie sind den Behörden überlassen. Die Behörden müssen den Zweck des geplanten Datenabgleichs, die abzugleichenden Datensätze und die Verfahren zur Benachrichtigung der Betroffenen in der Vereinbarung festlegen.

Für die Durchsetzung der Rasterfahndung sind gesetzlich verschiedene Schwellen festgelegt, indem zureichende tatsächliche Anhaltspunkte für Katalogtaten von erheblicher Bedeutung, die Subsidiarität einer Rasterfahndung und der Richtervorbehalt angefordert werden. Demgegenüber ist in den USA nur die behördenübergreifende Datenübermittlung zum Zweck des Datenabgleichs von einer Zustimmung der Betroffenen und dem Bedürfnis einer schriftlichen Vereinbarung abhängig. Es ist aber zweifelhaft, ob die Anforderungen als tatsächliche Schwellen funktionieren können, weil die Bedeutung einer Zustimmung der Betroffenen schwach ist und die schriftliche Vereinbarung inhaltlich nicht gesetzlich geregelt wird.

d) Aufbewahrungsdauer der Daten

Die deutsche Rechtsordnung sieht angesichts der Missbrauchsgefahr und der großen Bedeutung personenbezogener Daten in der modernen Gesellschaft eine maximale Aufbewahrungsdauer der Daten vor. So sind die erhaltenen Datenträger nach Beendigung des Abgleichs unverzüglich an die betreffenden Speicherstellen zurückzugeben und Daten, die auf andere Datenträger übertragen wurden, sind unverzüglich zu löschen, sobald sie für das Strafverfahren nicht mehr benötigt werden.

Die Aufbewahrungsdauer der Daten, die zum Zweck des Datenabgleichs übermittelt wurden, wird in der US-amerikanischen Regelung hingegen nicht berücksichtigt. Es obliegt den betroffenen Behörden, die Aufbewahrungsfristen oder die Rückgabe-, Löschungs- oder Vernichtungszeiten von Daten nach der Beendigung des Datenabgleichs festzulegen.

e) Mitteilungspflicht

Die deutsche Strafprozessordnung statuiert die Pflicht zur nachträglichen Unterrichtung der betroffenen Personen und des zuständigen Datenschutzbeauftragten. Die nachträgliche Unterrichtung der betroffenen Personen wird aber nur auf die Personen eingeschränkt, gegen die nach Abgleich der Daten weitere Ermittlungen geführt wurden. Die Unterrichtung

des zuständigen Datenschutzbeauftragten erfolgt erst nach Beendigung der Rasterfahndung. Personen, die zwar in eine Rasterfahndung einbezogen waren, aber gegen die keine weiteren Ermittlungen geführt wurden, werden nicht benachrichtigt. Die nachträgliche Unterrichtung des zuständigen Datenschutzbeauftragten kann außerdem mangels der Möglichkeit der Vorabunterrichtung, der Beratung und der begleitenden Kontrolle die effektive Kontrolle des Datenschutzes nicht garantieren.

In den USA werden die betroffenen Personen zur Gewährleistung der Anfechtungschance des Einzelnen benachrichtigt, wenn aufgrund der Ergebnisse des Datenabgleichs Leistungen reduziert oder gekündigt werden, also wenn eine nachteilige Entscheidung aufgrund der Ergebnisse des Datenabgleichs erwartet wird. Die Benachrichtigung ist mit einer möglichen nachteiligen Entscheidung nach Beendigung des Datenabgleichs, aber nicht mit dem Datenabgleich als solchem durchgeführt. Personen, gegen die keine nachteilige Entscheidung nach Beendigung des Datenabgleichs erwartet wird, werden nicht benachrichtigt. Mit der Pflicht zur Vorabeinbringung der schriftlichen Vereinbarung an einen zuständigen Ausschuss des Kongresses und zur Einrichtung des Datenaufsichtsausschusses mit Berichtspflicht innerhalb jeder Behörde ist die Möglichkeit der Vorabunterrichtung, Beratung und begleitenden Kontrolle garantiert.[643]

Tabelle 5: Gesetzliche Ausgestaltungen des Datenabgleichs in den beiden Ländern

	Anwendungsbereich	Voraussetzungen	Spezifische Kontrolle
Deutschland	§ 98a StPO Behördlicher computergestützter Datenabgleich mit polizeiexternen Dateien	Straftat von erheblicher Bedeutung; ergänzt durch typisierenden Katalog	Richtervorbehalt (staatsanwaltschaftliche Eilanordnungsmöglichkeit); Unterrichtung des Betroffenen; Unterrichtung des Datenschutzbeauftragten

643 Einen anschaulichen Vergleich des Datenabgleichs in den beiden Ländern siehe Tabelle 5.

USA	Behördlicher computergestützter Datenabgleich nur mit bei öffentlichen Stellen gespeicherten Dateien	Prozedurale Blankettnorm Zustimmung des Betroffenen für Zweckentfremdungsnutzung von Daten	Matching Agreement; Information an den Kongress; Errichtung eines Datenaufsichtsausschusses

III. Vorratsdatenspeicherung

1. Deutschland

a) Geschichtlicher Hintergrund

Nach § 12 FAG[644] und § 5 TDSV[645] wurde es möglich, Auskunft über bestimmte Verbindungsdaten zu verlangen. Ausschließlich damit konnte die Erhebung von bei einer Anordnung schon gelöschten bzw. nicht gespeicherten vergangenen Verbindungdaten jedoch nicht garantiert werden. Als Reaktion darauf wurden sowohl in Deutschland als auch auf europäischer Ebene mehrfach Versuche unternommen, die Telekommunikationsanbieter gesetzlich zur vorrätigen Speicherung bestimmter Verbindungsdaten zu verpflichten, aber diese Versuche scheiterten. Die gesetzliche Verpflichtung vorrätiger Speicherung bestimmter Verbindungsdaten in Deutschland gelang als Umsetzungspflicht der Vorratsdatenspeicherungsrichtlinie auf europäischer Ebene, die als Reaktion auf eine Reihe von Terroranschlägen erlassen wurde.[646]

Auf europäischer Ebene werden nicht nur das Recht auf Privatsphäre, sondern auch das Recht auf Schutz der sie betreffenden personenbezogenen Daten sowohl im Primärrecht als auch im Sekundärrecht ausdrücklich

644 Das Gesetz über Fernmeldeanlagen vom 3. Juli 1989 (BGBl. I S. 1455). Siehe auch oben Fn. 206.

645 Verordnung über den Datenschutz bei Dienstleistungen der Deutschen Bundespost TELEKOM (Telekom-Datenschutzverordnung) vom 24. Juni 1991, BGBl. 1991, I. S. 1391.

646 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. EU Nr. L 105, S. 54–60.

anerkannt und geschützt. Vor allem bildet die Datenschutzrichtlinie[647] die Grundsätze bei der Verarbeitung von personenbezogenen Daten: dass die Datenerhebung verhältnismäßig zum jeweiligen Zweck ist; dass die Datenerhebung in der Regel die Zustimmung des Betroffenen voraussetzt; dass die Verarbeitung sensibler Daten grundsätzlich verboten ist. Durch die Richtlinie 2002/58/EG[648] und die Verordnung 45/2001/EG[649] werden darüber hinaus die Grundsätze der Datenschutzrichtlinie im Bereich der elektronischen Kommunikation aktualisiert und die Rechtsvorschriften der Mitgliedstaaten zur Sicherstellung eines gleichwertigen Schutzniveaus der Grundrechte und Grundfreiheiten harmonisiert. Diese Harmonisierungsbemühungen haben aber wenig Wirkung, da die Datenschutzregelungen in der Europäischen Union immer noch viel dem Ermessen der Mitgliedstaaten überlassen. Dies hat zu den verschiedenen nationalen Gesetzen bezüglich des Datenschutzes geführt. Um diesen großen Unterschied zu vermeiden, wurde die Vorratsdatenspeicherungsrichtlinie[650] mit dem Ziel verabschiedet, diese verschiedenen nationalen Gesetze miteinander in Einklang zu bringen. Damit wurde die Verpflichtung der Mitgliedstaaten, bestimmte Daten auf Vorrat zu speichern, vorgesehen. Die Vorratsdatenspeicherungsrichtlinie zielt auf die Harmonisierung mitgliedstaatlicher Vorschriften über Vorratsdatenspeicherung und die Sicherstellung bestimmter Daten für die Ermittlung, Feststellung und Verfolgung schwerer Straftaten ab. Dafür werden die zu speichernden Daten und die Verwendungszwecke abschließend geordnet. Unter der Vorratsdatenspeicherung werden die Daten für eine eventuelle Anfrage mindestens sechs

---

647 Die Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr, 23. November 1995 (ABl. EG Nr. L 281 S. 31–50).

648 Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation, 31. Juli 2002 (ABl. EG Nr. L 201 S. 37–47).

649 Verordnung (EG) Nr. 45/2001 vom 18. Dezember 2000 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten durch die Organe und Einrichtungen der Gemeinschaft und zum freien Datenverkehr.

650 Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. EU Nr. L 105.

Monate und höchstens zwei Jahre ab dem Zeitpunkt der Kommunikation auf Vorrat gespeichert.

Gegen die Vorratsdatenspeicherungsrichtlinie wurde zweimal Beschwerde eingereicht: zuerst wegen der Frage der Wahl der Rechtsgrundlage und danach wegen der Frage der Vereinbarkeit der Richtlinie mit den EU-Grundrechten. Die erste Klage wurde mit der Begründung abgewiesen, dass sich die Regelungen zur Vorratsdatenspeicherung „unmittelbar auf das Funktionieren des Binnenmarkts auswirken und die Richtlinie Tätigkeiten regelt, die unabhängig von der Durchführung jeder eventuellen Maßnahme polizeilicher oder justizieller Zusammenarbeit in Strafsachen sind, damit sie die Dienstanbieter verpflichtet, bestimmte Daten auf Vorrat zu speichern“[651]. Die Frage über die Vereinbarkeit der Richtlinie mit den EU-Grundrechten wurde in der Vorabentscheidung des irischen High Court und des österreichischen Verfassungsgerichtshofs vorgelegt. Der EuGH erklärte dabei die Richtlinie für ungültig, weil sich die Ausnahmen vom Schutz personenbezogener Daten und dessen Einschränkung auf das absolut Notwendige beschränken müssen, aber die in der Richtlinie vorgesehene Verpflichtung der Telekommunikationsanbieter nicht auf das Notwendige beschränkt gewesen sei.[652] Das Problem liege darin, die Daten aller Personen anlassunabhängig in umfassender Weise zu speichern, keine Einschränkung auf konkrete schwere Straftaten vorzusehen und die Speicherungsdauer unabhängig von den unterschiedlichen Datenkategorien zu bestimmen.[653] Auch in den weiteren Vorabentscheidungsverfahren hat der EuGH klargestellt, dass eine nationale Regelung, die eine allgemeine Speicherung von Daten ohne ausreichende begrenzende Kriterien zulässt, nicht mit dem Unionsrecht vereinbar sei.[654] Mit den Urteilen des EuGHs wird betont, dass eine ausnahmslose, alle Kommunikationsteilnehmer erfassende Vorratsdatenspeicherung, ohne dass jene Personen einen Anlass dazu gegeben haben, mit dem Europarecht nicht vereinbar ist und dass die Vorratsdatenspeicherung hinsichtlich der Art der Daten, der betroffenen Kommunikationsmittel sowie der betroffenen Personen und der Speicherungsdauer auf das absolut Notwendige zu beschränken ist.

651 EuGH, C-301/06, 10.2.2009, Rn. 71 und 82 f.
652 EuGH, C-293/12, 8.4.2014, Rn. 52 und 65.
653 EuGH, C-293/12, 8.4.2014, Rn. 58, 60 und 63.
654 EuGH, C-203/15, C-698/15, 21.12.2016.

Die Richtlinie wurde im Jahr 2007 in das deutsche Recht aufgenommen,[655] bevor der EuGH sie für ungültig erklärte. Dabei wurde das Doppeltürmodell gewählt. Die Ermächtigungsgrundlage zur Verwendung der Daten im Rahmen der Strafverfolgung ist in der StPO und die konkrete Verpflichtung der Telekommunikationsanbieter im TKG vorgesehen. Der durch die Umsetzung der Vorratsdatenspeicherungsrichtlinie neu eingeführte § 113a TKG a. F. forderte, dass die unterschiedlichen Datenkategorien je nach der angebotenen Dienstleistung sechs Monate lang gespeichert werden, dass die erforderlichen Maßnahmen zur Sicherstellung der Qualität und des Schutzes der gespeicherten Daten ergriffen werden und dass die gespeicherten Daten innerhalb eines Monats nach Ablauf der Speicherungsfrist zu löschen sind. § 113b TKG a. F. bestimmte hier die Verwendungszwecke und die Verlangens- und Übermittlungsvoraussetzungen der Daten. Mit dem § 100g StPO wurden die Voraussetzungen vorgesehen. Danach dürften ohne Wissen des Betroffenen Verkehrsdaten erhoben werden, soweit dies für die Erforschung des Sachverhalts oder die Ermittlung des Aufenthaltsortes des Beschuldigten erforderlich ist, wenn bestimmte Tatsachen den Verdacht begründen, dass jemand als Täter oder Teilnehmer eine Straftat von auch im Einzelfall erheblicher Bedeutung, insbesondere eine in § 100a Abs. 2 bezeichnete Straftat oder eine Straftat mittels Telekommunikation, begangen hat. Bei einer Straftat mittels Telekommunikation wurden gesetzlich die Subsidiarität und die Verhältnismäßigkeit gefordert.

Das Umsetzungsgesetz ist auf Kritik gestoßen, die aus verfassungsrechtlichen Bedenken hervorging. Aufgrund von zahlreichen Verfassungsbeschwerden hat das Bundesverfassungsgericht mit seinem Urteil vom 2. März 2010 festgestellt, dass die §§ 113a und 113b des Telekommunikationsgesetzes in der Fassung des Artikels 2 Nummer 6 des Gesetzes zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG vom 21. Dezember 2007 gegen Artikel 10 Abs. 1 des Grundgesetzes verstoßen und nichtig sind und dass 100g Abs. 1 Satz 1 der Strafprozessordnung, soweit danach Verkehrsdaten nach § 113a TKG erhoben werden dürfen, auch gegen Artikel 10 Absatz 1 des Grundgesetzes verstößt und insoweit

655 Gesetz zur Neuregelung der Telekommunikationsüberwachung und anderer verdeckter Ermittlungsmaßnahmen sowie zur Umsetzung der Richtlinie 2006/24/EG, vom 21. Dezember 2007 BGBl. I S. 3198 (Nr. 70); Geltung ab 01. Januar 2008.

nichtig ist.[656] Nach der Entscheidung sei die Vorratsdatenspeicherung zwar nicht schlechthin mit dem Grundgesetz unvereinbar und nicht von vornherein unverhältnismäßig im engeren Sinn, aber die Regelungen entsprechen nicht den verfassungsrechtlichen Anforderungen. Das Bundesverfassungsgericht forderte diesbezüglich die gesetzliche Gewährleistung eines besonders hohen Standards der Datensicherheit, die eng beschränkten sowie konkreten gesetzlichen Regelungen über die Voraussetzungen für die Datenverwendung und deren Umfang und die hinreichenden Vorkehrungen zur Transparenz der Daten sowie zur Gewährleistung eines effektiven Rechtsschutzes und effektiver Sanktionen.

Trotz der Tatsache, dass die Vorratsdatenspeicherung durch das Bundesverfassungsgericht für nichtig erklärt wurde, hat das praktische Sehnen nach ihr im Jahr 2015 zur erneuten Verabschiedung des Gesetzes zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten geführt. Der Erlass dieses Gesetzes rührt nicht von der Umsetzungspflicht innerhalb der Europäischen Union her. Das Gesetz ist nach den Anforderungen des Bundesverfassungsgerichts von der abschließenden Aufzählung der Straftaten flankiert, bei denen die nach § 113b TKG gespeicherten Daten erhoben werden, und den Vorkehrungen zur Datensicherheit und zur Transparenz der Datenverwendung. Gegen das Gesetz haben sich erneut Antragsteller mit Anträgen auf Erlass einer einstweiligen Anordnung gewandt. Die Anträge wurden vom Bundesverfassungsgericht zwar abgelehnt. Hinsichtlich der verfassungsrechtlichen Bewertung der angegriffenen Regelungen stellen sich jedoch immer noch Fragen, die nicht zur Klärung im Eilrechtsschutzverfahren geeignet sind. Anschließend haben das Oberverwaltungsgericht für das Land Nordrhein-Westfalen[657] und das Verwaltungsgericht Köln[658] bei weiteren Klagen die Unvereinbarkeit des Gesetzes mit dem Unionsrecht erklärt. Das Bundesverfassungsgericht hat jedoch eine Aussetzung des Vollzugs der §§ 113a und 113b TKG sowie §§ 100g, 101a und 101b StPO ausdrücklich abgelehnt.[659] Eine Entscheidung der Hauptsache ist noch abzuwarten. Das geltende Gesetz zur Einführung einer Speicherpflicht und Höchstspeicherfrist für Verkehrsdaten ist jedenfalls bis zur endgültigen Entscheidung des Bundesverfassungsgerichts immer noch gültig.

656 BVerfGE 125, 260.
657 OVG NRW, 13 B 238/17.
658 VG Köln, 9 K 7417/17.
659 BVerfG, 08.06.2016, 1 BvQ 42/15, NVwZ 2016, 1240.

b) Aktuelle Rechtslage

Die Systematik der Vorratsdatenspeicherung gründet sich mit der Begründung der Speicherpflicht sowie der Bestimmung der Verantwortlichen und sonstiger Parameter im TKG und der korrespondierenden Zugriffsnorm für den Abruf durch die Strafverfolgungsbehörden in der StPO auf das Doppeltürmodell.[660] Da die Erhebung, Verarbeitung und Nutzung personenbezogener Daten nach dem BDSG grundsätzlich verboten sind, sind das TKG und die StPO hier die Ermächtigungsnormen. Der Diensteanbieter der Telekommunikation darf prinzipiell gemäß § 95 TKG Bestandsdaten eines Teilnehmers, die für die Begründung, inhaltliche Ausgestaltung, Änderung oder Beendigung eines Vertragsverhältnisses über Telekommunikationsdienste erhoben werden, und gemäß § 96 TKG bestimmte Verkehrsdaten zur Ermittlung des Entgelts und zur Abrechnung mit ihren Teilnehmern erheben und verwenden. Außerdem dürfen Standortdaten, die in Bezug auf die Nutzer von öffentlichen Telekommunikationsnetzen oder öffentlich zugänglichen Telekommunikationsdiensten verwendet werden, nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Umfang und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer dem Anbieter des Dienstes mit Zusatznutzen seine Einwilligung erteilt hat. Unabhängig von dieser üblichen Datenerhebung und -verwendung hat der Diensteanbieter gemäß § 111 TKG zusätzlich für die Auskunftsverfahren nach den §§ 112 und 113 die Rufnummern und andere Anschlusskennungen, den Namen und die Anschrift des Anschlussinhabers, bei natürlichen Personen deren Geburtsdatum, bei Festnetzanschlüssen zudem die Anschrift des Anschlusses, in Fällen, in denen neben einem Mobilfunkanschluss auch ein Mobilfunkendgerät überlassen wird, die Gerätenummer dieses Gerätes sowie das Datum des Vertragsbeginns vor der Freischaltung zu erheben und unverzüglich zu speichern, auch wenn diese Daten nicht für betriebliche Zwecke erforderlich sind. Vor der Einführung der Vorratsdatenspeicherung durfte die Strafverfolgungsbehörde nach den §§ 100g und 100j StPO nur die nach den §§ 95, 96 und 111 TKG beim Diensteanbieter gespeicherten Daten und die Standortdaten nur für künftig anfallende Verkehrsdaten oder in Echtzeit erheben.

Vor der Einführung der Vorratsdatenspeicherung waren die Verkehrsdaten, die die Strafverfolgungsbehörde erheben darf bzw. kann, sehr eingeschränkt. Aber nach der Einführung der Vorratsdatenspeicherung werden

660 *Dalby*, Vorratsdatenspeicherung – Endlich?! KriPoZ 2016, 113, 113.

die Verkehrsdaten, die der Diensteanbieter zu speichern verpflichtet ist, erweitert und die Übermittlung dieser Daten wird abgesichert. Zugleich werden mehrere Maßnahmen getroffen, die die hohe Eingriffsintensität der Vorratsdatenspeicherung abfedern können.

aa) Zu speichernde Daten

Erbringer öffentlich zugänglicher Telekommunikationsdienste sind nach der Vorratsdatenspeicherung dazu verpflichtet, bestimmte Verkehrsdaten zu speichern. § 113b Abs. 2 bis 4 TKG beschreibt abschließend die Verkehrsdaten und die Standortdaten, die von den Erbringern öffentlich zugänglicher Telefon- und Internetzugangsdienste zu speichern sind.

§ 113b Abs. 2 regelt die einzelnen Speicherpflichten für Erbringer öffentlich zugänglicher Telefondienste. Er umfasst Ausprägungen wie Festnetz, Mobilfunk und Internettelefonie. Erbringer von Telefondiensten haben die folgenden Daten zu speichern: Rufnummer oder eine andere Kennung des anrufenden und des angerufenen Anschlusses sowie bei Um- oder Weiterschaltungen jedes weiteren beteiligten Anschlusses, Datum und Uhrzeit von Beginn und Ende der Verbindung sowie Angaben zu dem genutzten Dienst. Die Erbringer mobiler Telefondienste haben zusätzlich die internationale Kennung des anrufenden und des angerufenen Endgerätes sowie Datum und Uhrzeit der ersten Aktivierung des Dienstes im Fall von Prepaid-Angeboten zu speichern. Im Fall von Internet-Telefondiensten wird auch die Speicherung der Internetprotokoll-Adressen des anrufenden und des angerufenen Anschlusses sowie der zugewiesenen Benutzerkennungen verlangt. Die Speicherpflicht erstreckt sich auf unbeantwortete oder wegen eines Eingriffs des Netzwerkmanagements erfolglose Anrufe. Damit werden beispielsweise Fälle erfasst, in denen ein Teilnehmer von seinem Diensteanbieter per Kurznachricht darüber informiert wird, dass ein für seinen Anschluss bestimmter Anruf nicht entgegengenommen wurde, etwa weil der Anschluss belegt war oder sich das Mobiltelefon zur Zeit des Anrufs außerhalb des Versorgungsbereichs einer Funkzelle befand.[661]

Erbringer öffentlich zugänglicher Internetzugangsdienste haben die dem Teilnehmer für eine Internetnutzung zugewiesene Internetprotokoll-Adresse, eine eindeutige Kennung des Anschlusses, über den der Internetzugang erfolgt, sowie eine zugewiesene Benutzerkennung sowie Datum und Uhrzeit von Beginn und Ende der Internetnutzung unter der zugewie-

661 BT-Drs. 18/5088, S. 39.

senen Internetprotokoll-Adresse zu speichern.[662] Hier findet eine Speicherung der im Internet aufgerufenen Adressen nicht statt, damit auch auf Grundlage der zu speichernden Internetdaten nicht das gesamte Surfverhalten von Internetnutzern nachvollziehbar wird.[663]

Darüber hinaus sind im Fall der Nutzung mobiler Telefondienste die Standortdaten des anrufenden und des angerufenen Anschlusses bei Beginn der Verbindung, also die konkreten Bezeichnungen der Funkzellen, zu speichern, über die die Telekommunikationsteilnehmer beim Verbindungsaufbau versorgt werden. Bei der Nutzung von öffentlich zugänglichen Internetzugangsdiensten durch Mobilfunk wird die Bezeichnung der Funkzelle gespeichert, die bei Beginn der Internetverbindung genutzt wird. In beiden Fällen sind zusätzlich die Daten vorzuhalten, aus denen sich die geografische Lage und die Hauptstrahlrichtungen der die jeweilige Funkzelle versorgenden Funkantennen ergeben. Dies begründete der Gesetzgeber damit, dass die Funkzellen von den Erbringern öffentlich zugänglicher Telekommunikationsdienste nicht dauerhaft zugewiesen werden und die Angabe der Hauptstrahlrichtungen der einzelnen Funkantennen der Ermöglichung einer genauen Ermittlung des Standortes dient, von dem aus oder zu dem eine Telekommunikationsverbindung aufgebaut wurde.[664]

Ein merkwürdiger Aspekt der Vorratsdatenspeicherung ist vor allem, dass eine solche Datenspeicherung nicht durch einen Anlass hervorgerufen wird. Ohne dass ein Anlass zur Speicherung der in § 113b TKG genannten Daten erforderlich ist, werden die Daten aller Bürger für eventuelle Anfragen vorrätig gespeichert. Zur Speicherung dieser Daten wird weder ein Zusammenhang mit schweren Straftaten noch eine Zweckbeschränkung gefordert. Trotz erheblicher Bedenken bezüglich der Eingriffsintensität der

662 *Dalby* hält die Speicherpflicht für dynamische IP-Adressen für begrüßenswert. Für Bestandsdatenauskünfte zu dynamischen IP-Adressen darf nach § 113b TKG auf gespeicherte Verkehrsdaten zurückgegriffen werden. Zwar war bereits vorher ein Pool dynamischer IP-Adressen abfrag- und zuordenbar, doch die Speicherung dieser dynamischen IP-Adressen auf Grundlage der §§ 96 ff. TKG war hochstreitig, weil das Diensteunternehmen diese nicht für Abrechnungszwecke bei der heutigen Verbreitung von Flatrate-Tarifen benötigt: *Dalby*, Vorratsdatenspeicherung – Endlich?!, KriPoZ 2016, 113, 116.

663 BT-Drs. 18/5088, S. 39. Das Bundesverfassungsgericht befürchtete in seinem Volkszählungsurteil die Gefahr eines umfassenden und detaillierten Bildes der jeweiligen Person – einer Herstellung von Persönlichkeitsprofilen: BVerfGE 65, 1 (17, 25).

664 BT-Drs. 18/5088, S. 39.

anlasslosen Speicherung[665] behauptet der Gesetzgeber die Minderung der Eingriffsintensität durch verschiedenste Anforderungen.[666]

bb) Zugriff auf Daten

Eine verpflichtend anlassunabhängige Datenspeicherung durch den Anbieter öffentlich zugänglicher Telekommunikationsdienste ergänzt sich durch die strengen Abrufmechanismen. Auf die nach der Vorratsdatenspeicherung gespeicherten Daten darf unter strikteren Voraussetzungen zugegriffen werden als auf die Daten, die gemäß § 96 TKG gespeichert sind. Der Unterschied beruht auf dem Risiko der Grundrechtsbeeinträchtigung der anlasslosen Speicherung der Vielzahl von Daten Unbeteiligter.

Das Telekommunikationsgesetz, das die Vorratsdatenspeicherung vorsieht, schränkt mit § 113c den Verwendungszweck der Vorratsdaten ein. Für den Zugriff auf die Daten zur Verfolgung besonders schwerer Straftaten werden ein Verdacht einer Katalogtat im Sinne des § 100g Abs. 2 Satz 2 Nr. 1–8 StPO, die auch im Einzelfall besonders schwer wiegt, die Erforderlichkeit zur Sachverhaltserforschung oder zur Aufenthaltsermittlung und die besondere Verhältnismäßigkeit vorausgesetzt. Hier sind also eine Einschränkung auf eine der Katalogstraftaten als eine Anlasstat zum Zugriff auf die Daten, die wesentliche Erschwernis oder die Erfolgsaussichten anderer Maßnahmen und die besondere Verhältnismäßigkeit dafür erforderlich, dass sich die Ausnahmen zum Schutz personenbezogener Daten und dessen Einschränkungen auf das absolut Notwendige beschränken müssen. Alle Voraussetzungen gelten auch für die Erhebung aller Verkehrsdaten (sog. Funkzellenabfrage), die in einer bestimmten Funkzelle angefallen und nach § 113b TKG gespeichert sind. Im Vergleich zu der Erhebung der Vorratsdaten des bekannten Verdächtigen wäre bei einer Funkzellenabfrage, die die Telekommunikationsdaten völlig unbeteiligter Personen erheben lässt, die Gefahr einer Grundrechtsbeeinträchtigung viel höher. Dieser unterschiedliche Grad der Gefahr kommt aber gesetzlich nicht in Betracht.

Der Datenerhebung nach § 100g StPO muss eine richterliche Anordnung vorausgehen. Richtigerweise ist für die Erhebung der nach § 113b

665 Bejahend *Dalby*, Vorratsdatenspeicherung – Endlich?!, KriPoZ 2016, 113, 116; kritisch dazu *Roßnagel*, Die neue Vorratsdatenspeicherung – der nächste Schritt im Ringen um Sicherheit und Grundrechtsschutz, NJW 2016, 533, 538.

666 BT-Drs. 18/5088, S. 39.

TKG gespeicherten Daten die Möglichkeit der Anordnung der Staatsanwaltschaft bei Gefahr im Verzug ausgeschlossen.

Die Weitergabe der Daten, die durch Maßnahmen nach § 100g Abs. 2 StPO, auch in Verbindung mit § 100g Abs. 3 Satz 2, erhoben wurden, ist unter dem Zweckbindungsgrundsatz nach § 101a Abs. 4 eingeschränkt zulässig. Diese Daten dürfen also ohne Einwilligung der Beteiligten der betroffenen Telekommunikation in anderen Strafverfahren zur Aufklärung einer Straftat, aufgrund derer eine Maßnahme nach § 100g Absatz 2, auch in Verbindung mit § 100g Absatz 3 Satz 2, angeordnet werden könnte, oder zur Ermittlung des Aufenthalts der einer solchen Straftat beschuldigten Person, verwendet werden.

Der Gesetzgeber versucht damit, die Gefahr einer Grundrechtsbeeinträchtigung durch eine verpflichtende Speicherung bestimmter Daten aller Bürger mit einer strikten Einschränkung der Voraussetzungen der Datenverwendung und -weitergabe aufzurechnen.

cc) Löschungspflicht

Die Speicherung der Verkehrsdaten, die grundsätzlich nach dem BDSG verboten, jedoch nach dem TKG ausnahmsweise zulässig ist, erfolgt nicht auf unbestimmte Zeit. Zum Schutz personenbezogener Daten und zur Minderung der Eingriffsintensität der Vorratsdatenspeicherung sieht das TKG eine bestimmte Speicherungsfrist vor. Bei der Bestimmung der Speicherungsfrist kommt die unterschiedliche Bedeutung verschiedener Daten in Betracht. Die nach der Vorratsdatenspeicherung gespeicherten Daten müssen nach maximal zehn Wochen irreversibel gelöscht werden. Hingegen erfordert das TKG keine Löschung oder Rückgabe für die vom Diensteanbieter bereits an eine zuständige Behörde übermittelten Daten. Denn die nach einer gerichtlichen Anordnung erhaltenen Daten, die vom Gericht unter einer hinreichenden Erörterung der Angemessenheit der Maßnahme zur Ermittlung erteilt wird, dürfen aufgrund einer engen Zweckbegrenzung für die Verwendung dieser Daten nicht für andere Zwecke verwendet werden.

dd) Mitteilungspflicht

Zum Rechtsschutz des Einzelnen wird eine Benachrichtigung an die Beteiligten der betroffenen Telekommunikation grundsätzlich vor der Erhe-

bung der Verkehrsdaten nach § 100g StPO garantiert. Aber die Benachrichtigung kann ausnahmsweise zurückgestellt werden oder unterbleiben, wenn das öffentliche Interesse überwiegt. Das Unterbleiben oder die Zurückstellung der Benachrichtigung ist nur auf Anordnung des zuständigen Gerichts zulässig.

2. USA

a) Geschichtlicher Hintergrund

Eine vorrätige und anlasslose Speicherung bestimmter Daten für eine eventuelle Ermittlung ist in den US-amerikanischen Gesetzen nicht zu finden. Zwar wurde die Einführung dieser Speicherungspflicht im Parlament mehrmals versucht, aber ihre Gesetzgebung konnte kein einziges Mal verwirklicht werden. Das Scheitern kann auf zwei Gründe zurückgeführt werden. Ein Grund ist das fehlende Datenschutzgesetz im Privatsektor. Da es kaum Einschränkungen der Datenspeicherungspraxis im Privatsektor gibt, kann ein privates Unternehmen ohne weitere Einschränkungen ungeheure Daten speichern und diese soweit es das will auch verarbeiten. Der Staat sorgt sich relativ wenig darum, ob die Daten zum Anfragezeitpunkt nicht oder nicht mehr gespeichert sind.

Ein anderer Grund liegt in den Erfahrungen mit der staatlichen Datenspeicherungspraxis im Laufe der Geschichte. Die Antidrogenbehörde DEA hat zwanzig Jahre lang Milliarden von Telefonverbindungsdaten gespeichert. Sie hat nur mit der administrativen *subpoena* von Telefonanbietern die Listen aller Anrufe aus den USA ins Ausland erhalten und erforderlichenfalls an andere Behörden weitergeleitet. Diese Anfangsdaten, die Hinweise für die Ermittlung geben, wurden durch die *parallel construction* abgedeckt. Diese Speicherungspraxis durch die DEA wird auf verschiedene Weisen von der NSA fortgesetzt. Da die Praxis der Metadatensammlung der NSA vor der Snowden-Offenlegung kaum bekannt war, wurden die Datensammlungs- und Datenverwendungsbefugnisse der NSA unter verdeckten Programmen missbraucht. Um den Missbrauch zu verhindern, wurde der Foreign Intelligence Surveillance Act (FISA) erlassen und der FISA-Court etabliert. Das Gesetz setzt für eine Datensammlung einen *probable cause* voraus. Der *probable cause* bezieht sich darauf, dass das Ziel der elektronischen Überwachung eine ausländische Macht oder ein Vertreter einer ausländischen Macht ist und dass sich die gesuchten Informationen auf die nationale Sicherheit beziehen, aber nicht auf einen Anlass dazu

oder auf einen Verdacht darauf, dass das Ziel ein Verbrechen begangen hat oder begehen wird. Der Datenaustausch zwischen dem Geheimdienst und der Strafverfolgungsbehörde wurde blockiert, damit eine Negierung der Notwendigkeit einer rechtmäßigen Titel-III-Anordnung und eine Umgehung ihrer Voraussetzungen vermieden werden.

Die Terroranschläge vom 11. September 2001 haben vieles verändert. Eine der Veränderungen war die Erweiterung der Befugnisse der NSA durch den PATRIOT Act. Mit diesem Gesetz konnten Telekommunikationsunternehmen unter bestimmten Bedingungen freiwillig Kommunikations- und Standortdaten an die Strafverfolgungsbehörden übergeben. Die Datenarten, die mit einer *subpoena* erhoben werden können, wurden ebenfalls erweitert. Außerdem wurde die Mauer zwischen den Nachrichtendienst- und den Strafverfolgungsbehörden durchbrochen. Der Abschnitt 215 PATRIOT Act eröffnete die Möglichkeit, vor dem FISC eine geheime gerichtliche Anordnung zu beantragen. Der Abschnitt 215 stellte auch die parlamentarische Kontrolle für das FISA-Programm zur Verfügung. Trotz der erweiterten Möglichkeit einer geheimen gerichtlichen Anordnung meinte die Regierung, dass sie aufgrund der Third-Party-Doktrin auch ohne gerichtliche Anordnungen Daten erheben darf. Unter diesen Umständen hat die NSA anlasslos und ohne einen Verdacht Listen mit allen Anrufen erhoben.

Die Massentelefoniemetadatensammlung durch die NSA wurde erst durch die Enthüllung des ehemaligen NSA-Mitarbeiters Snowden entdeckt. Die Massenüberwachung wurde zwar mit einigen Sicherungen wie etwa einer gerichtlichen sowie einer parlamentarischen Kontrolle und den *minimization procedures*,[667] die durch den FISA eingeführt wurden, in gewissem Maße begrenzt. Die Speicherpraxis der NSA ist jedoch wegen der einseitigen Vorlegung der Daten durch die Regierung als Grundlage der Entscheidung des FISC, des Zusammenbruchs der Mauer zwischen Nachrichtendienst- und Strafverfolgungsbehörden, der Erweiterung der Befugnisse der NSA und der Third-Party-Doktrin auf heftige Kritik gestoßen.

Nach dem Snowden-Skandal hat die Frage über die Rechtmäßigkeit und die Verfassungsmäßigkeit des Metadatensammlungsprogramms der NSA für Massentelefonie vor den Gerichten zu völlig unterschiedlichen

667 *Reid*, NSA and DEA Intelligence Sharing: Why it is legal and why REUTERS and the GOOD WIFE got it wrong, SMU Law Review, Vol. 68 Issue 2, 2015, S. 442 f.

Ergebnissen geführt.[668] Um das Problem der Rechtsunsicherheit zu lösen, wurde der Freedom Act[669] erlassen. Das Gesetz stellt das Metadatensammlungsprogramm der NSA in zweierlei Hinsicht unter strengere Voraussetzungen: zum einen gibt es eine Einschränkung des Mechanismus, zum anderen eine starke Forderung nach Datenverarbeitungstransparenz und öffentlicher Berichterstattung. Unter dem Gesetz muss die Einholung einer FISC-Anordnung für die Metadatensammlung erfolgen. Die Datensammlung ist keine allgemeine, sondern eine gezielte Sammlung von Telefonmetadaten. Nicht mehr die Regierung speichert die Daten, sondern auch das Unternehmen selbst. Es speichert die Verbindungsdaten für eventuelle Anfragen. Mit diesem Gesetz wurde die geheime Natur der FISA-Anordnung ausgeschlossen und die Möglichkeit der Benachrichtigung an den Betroffenen eröffnet. Angesichts dieser geschichtlichen Erfahrungen und der Umstände des fehlenden Datenschutzgesetzes wird in den USA keine Vorratsdatenspeicherung, sondern nur die anlassgebundene Datenspeicherung (das sog. Quick-Freeze-Verfahren) praktiziert.

b) Aktuelle Rechtslage

Um die absichtliche Überwachung kabelgebundener Kommunikationen ohne Einschränkung im Hinblick auf die aussagekräftige Bedeutung der Speicherung und der Nutzung von Telekommunikationsdaten zu verhindern, haben die USA im Jahr 1968 den Federal Wiretap Act[670] erlassen. Anschließend wurde das Gesetz durch den ECPA von 1986[671] geändert, damit auch die drahtlosen Kommunikationen erfasst werden können. Das ECPA besteht aus dem Wiretap Act, dem Stored Communications Act und dem Pen Register Act. Im Wiretap Act geht es um die Überwachung laufender Kommunikationen, im SCA um die Erhebung gespeicherter Kommunikationsdaten und im Pen Register Act um die Zulassungsbedingungen eines Geräts für die Ausspähung künftiger Kommunikationsdaten. Für einen bedeutungsvollen Vergleich konzentrierte sich die vorliegende Arbeit auf die Behandlung bereits gespeicherter oder künftig zu speichern-

668 Beispielsweise ACLU v. Clapper, 959 F. Supp. 2d 724 (S. D. N. Y. 2013); Klayman v. Obama, 957 F. Supp. 2d 1, 9 (D. D. C. 2013).

669 USA FREEDOM Act (the Uniting and Strengthening America by Fulfilling Rights and Ending Eavesdropping, Dragnet-collection and Online Monitoring Act), H. R. 3361, 113th Cong. (2013–2014).

670 Pub. L. 90-351, June 19, 1968, 82 Stat. 42 U. S. C. § 3711.

671 Pub. L. 99-508, October 21, 1986, 100 Stat. 1848.

der Kommunikationsdaten im SCA und Pen Register Act. Mit dem PATRIOT Act,[672] dem Freedom Act und dem Privacy Act werden der Zugang der Strafverfolgungsbehörden zu elektronischen Daten verbessert und der Datenschutz für die Verbraucher verringert. Das Gesetz ermöglicht das freiwillige Weitergeben von Verkehrs- und Bestandsdaten durch den Diensteanbieter der Telekommunikation an die Strafverfolgungsbehörden. Außerdem können mehr Daten von der Strafverfolgungsbehörde nur mit einer *subpoena* ohne Benachrichtigung des Betroffenen erhoben werden.

Die Systematik der US-amerikanischen Datenspeicherung stützt sich auf ein Verfahren, bei dem die Daten einer verdächtigen Person ab dem Zeitpunkt einer polizeilichen Anordnung gegen ein Telekommunikationsunternehmen erhoben und gespeichert werden (das sog. Quick-Freeze-Verfahren). Bei diesem Verfahren kann nur auf die zu und ab dem Zeitpunkt einer Anordnung noch vorhandenen und entstehenden Verbindungsdaten zugegriffen werden. Dabei ist der Diensteanbieter nach dem CALEA von 1994[673] dazu verpflichtet, seine Netze so auszulegen, dass er auf das befugte behördliche Überwachungsersuchen reagieren kann.

aa) Zu speichernde Daten

Es gibt weder eine Verpflichtung für die Erbringer öffentlich zugänglicher Telekommunikationsdienste, anlasslos bestimmte Daten vorrätig zu speichern, noch gibt es eine Aufzählung, in der eindeutig identifiziert wird, welche die zu speichernden Daten wären. Früher speicherte die NSA selbst die von den Telekommunikationsanbietern übertragenen Daten. Eine Speicherung liegt nun ausschließlich in der Hand der Telekommunikationsanbieter. Der ECPA schreibt nicht die zu speichernden Daten vor, sondern die Voraussetzungen für den Zugriff auf die Daten, die von Anbietern schon gespeichert wurden. Der Erfolg eines behördlichen Zugriffs hängt von der Speicherpraxis der Telekommunikationsunternehmen vor der berechtigten Aufbewahrungsanordnung ab, weil gesetzlich keine Speicherpflicht bestimmt ist. Die Abhängigkeit von der privaten Speicherpraxis kann möglicherweise die Effektivität der strafrechtlichen Ermittlungen nicht gefährden, wenn eine Erhebung, Speicherung und

672 Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (2001).

673 Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 U. S. C. §§ 1001–1010.

Verarbeitung personenbezogener Daten grundsätzlich erlaubt sind. Ein Verbot gilt nach dem ECPA nicht schon für die Speicherung der Daten, sondern erst für die Übermittlung der Daten. § 2703 Abs. a ECPA schreibt ein grundsätzliches Verbot der Übermittlung von Kommunikationsinhalten und Verkehrsdaten vor, § 2703 Abs. b und c eröffnet jedoch die Ausnahmemöglichkeit der Übermittlung von Kommunikationsinhalten und Verkehrsdaten.

Außerdem werden die Daten, auf die eine Behörde zugreifen darf, mit Ausnahme von Daten, auf die aufgrund einer *subpoena* zugegriffen wird,[674] gesetzlich nicht eingeschränkt, solange sich diese Daten noch im Besitz von Erbringern öffentlich zugänglicher Telekommunikationsdienste befinden. Der Diensteanbieter von Telekommunikationen ergreift nach § 2703 Abs. f auf Ersuchen einer staatlichen Stelle alle erforderlichen Maßnahmen, um die Verkehrsdaten und andere Beweismittel in seinem Besitz bis zur Erteilung eines Gerichtsbeschlusses oder eines anderen Verfahrens aufzubewahren. Dabei sichert der CALEA die Durchsetzung der anlassgebundenen Datenspeicherung, indem die Telekommunikationsunternehmen mit der Übermittlung der verfügbaren Telekommunikationsdaten an die zuständige Stelle beauftragt werden. Eine Aufbewahrung erfolgt auf der Basis eines *warrant* oder einer gerichtlichen Anordnung. Nur beim Vorliegen eines *probable cause* oder wenn die staatliche Stelle konkrete und verständliche Fakten vorlegt, aus denen hervorgeht, dass Grund zu der Annahme besteht, Kommunikationsinhalt, Verkehrsdaten oder sonstige Informationen seien für eine laufende strafrechtliche Untersuchung relevant und wesentlich, ist der Diensteanbieter dazu verpflichtet, diese Daten aufzubewahren. Hier ist weder ein Zusammenhang mit schweren Straftaten noch eine Zweckbeschränkung etwa zur Bekämpfung der organisierten Kriminalität erforderlich. Für eine Aufbewahrungsanordnung reicht es aus, den Zusammenhang mit der laufenden Untersuchung zu klären.

674 Eine Behörde kann die folgenden Daten, die mit den in Deutschland so genannten Bestandsdaten vergleichbar sind, auch allein mit einer *subpoena* erhalten: Namen, Adressen, Listen von Fernsprechanschlüssen, Daten über die Anzahl und die Dauer der Anrufe in einem bestimmten Zeitraum, die Dienstdauer (einschließlich des Anfangsdatums) und die Art der benutzten Dienste und Zahlungsmittel (einschließlich Kreditkarten- oder Bankkontonummer).

bb) Zugriff auf Daten

Für die Erhebung von Verkehrsdaten außer Inhaltsdaten, deren Speicherung eine staatliche Behörde vom Anbieter öffentlich zugänglicher Telekommunikationsdienste unter bestimmten Voraussetzungen anfordert, schränkt der ECPA den Verwendungszweck nicht ein, sondern sieht nur die Voraussetzungen vor, die die Datenverwendung ermöglichen. Die Verkehrsdaten dürfen entweder auf Basis der Zustimmung des Betroffenen oder eines *warrant* erhoben werden, eine gerichtliche Anordnung, die durch die Darstellung der spezifischen und klaren Tatsachen erworben wird, aus denen ersichtlich ist, dass Grund zu der Annahme besteht, die angeforderten Daten seien für eine laufende strafrechtliche Untersuchung relevant und wesentlich. Bestimmte Verkehrsdaten dürfen auch nur mit einem formellen schriftlichen Antrag oder einer *subpoena* erhoben werden. Der Diensteanbieter ist dabei nach dem CALEA dazu verpflichtet, die Behörde zu unterstützen. Damit wird die Datenübermittlung durch den Anbieter an die Behörde sichergestellt.

Während für die Verwendung eines Standorttrackers, der den Standort im mit bloßem Auge nicht sichtbaren Innenraum bekannt macht, ein *warrant* grundsätzlich vorausgesetzt wird, werden für die Standortdaten durch die Bezeichnungen der Funkzellen, die durch den anrufenden und den angerufenen Anschluss während der Verbindung genutzt werden, die erleichterten Voraussetzungen nach dem SCA angewendet.

Gesetzlich ist weder ein Verwendungszweck noch eine Zweckbindung erforderlich. Die Verkehrsdaten, die eine Behörde auf diese Weise erhoben hat, dürfen daher ohne Einschränkungen an eine andere Behörde weitergeleitet werden.

cc) Löschungspflicht

Als die notwendige Folge eines Mangels eines Datenschutzgesetzes im Privatsektor sind die Anbieter von Telekommunikationsdiensten nicht dazu verpflichtet, ihre Daten innerhalb eines bestimmten Zeitraums zu löschen oder zu vernichten. Den Telekommunikationsunternehmen wird gesetzlich nur ein Rat erteilt, die personenbezogenen Daten effektiv und sicher zu löschen, wenn die Unternehmen ihre Daten löschen wollen. Zur effektiven Strafverfolgung wird nicht die Regelung einer Löschungspflicht, sondern die Sicherstellung bestimmter Daten innerhalb eines bestimmten Zeitraums gewählt. Die Telekommunikationsunternehmen bewahren ihre

Daten in der Praxis in der Regel dreißig bis neunzig Tage auf.[675] 18 U. S. C. § 2703 (f) stellt dabei die Speicherung der Daten mindestens für neunzig Tage – die zusätzlich noch um neunzig Tage verlängert werden können – sicher. Die Vorschrift garantiert die Speicherung der Daten für diesen Zeitraum, aber nicht die Löschung der Daten nach diesem Zeitraum. Darüber hinaus ist die unterschiedliche Speicherungsdauer je nach der Bedeutung der angefragten Daten nicht vorgesehen.

Es gibt auch keine Löschungs- oder Übermittlungsverbotsvorschrift bezüglich der bereits bei einer Behörde liegenden Daten nach deren Verwendung. Bei der Datenverwendung wird ebenfalls keine strikte Zweckbegrenzung gefordert. Zwar wird die Datenübermittlung an eine andere Behörde nach dem Privacy Act an eine schriftliche Aufforderung oder Einverständniserklärung der Betroffenen gebunden, es scheint aber schwierig zu sein, die Datenverwendung für andere Zwecke einzuschränken. Dies liegt daran, dass eine gerichtliche Anordnung, die die Datenübermittlung vom Telekommunikationsunternehmen an eine zuständige Behörde ermöglicht, nur mit bestimmten und klaren Fakten erteilt wird, die eine vernünftige Grundlage für die Annahme darstellen, dass die geforderten Daten im Zusammenhang mit einer laufenden Untersuchung stehen.

dd) Mitteilungspflicht

Die Benachrichtigung an die Beteiligten der betroffenen Telekommunikation ist nach dem 18 U. S. C. § 2703 ausschließlich für die Erhebung von Telekommunikationsinhalten nicht durch einen *warrant*, sondern durch eine *subpoena* oder eine gerichtliche Anordnung erforderlich, aber nicht für die Erhebung von Verkehrsdaten. Der Betroffene nimmt also keine Kenntnis von der staatlichen Erhebung seiner Verkehrsdaten und kann folgerichtig keinen Anspruch auf den Schutz gegen eine unbefugte oder übermäßige Erhebung, Speicherung oder Verwendung seiner Daten erheben.

675 *Ringland*, The European Union's Data Retention Directive and the United States's Data Preservation Laws: Finding the Better Model, 5 Shidler J. L. Com. & Tech. 13, 2009; *McCullagh*, Gonzales Pressures ISPs on Data Retention, ZDNET News v. 27. Mai 2006, abrufbar unter: https://www.zdnet.com/article/gonzales-pressures-isps-on-data-retention/.

3. Vergleich

a) Geschichtlicher Hintergrund

Die Vorratsdatenspeicherung war in Deutschland inzwischen Widerspruch ausgesetzt: Mehrere Gesetzgebungsversuche waren gescheitert, das gelungene Gesetz wurde für nichtig erklärt und ein neues Gesetz zwar erneut erlassen, doch auch gegen dieses Gesetz wurden viele Einwände erhoben. Die praktische Erforderlichkeit der vorrätigen Datenspeicherung für eventuelle Anfragen wird teilweise anerkannt, wobei man angesichts der hohen Intensität des Eingriffs dieser Datenspeicherung viele Sicherungsmaßnahmen zum Privatsphären- oder Datenschutz des Einzelnen implementiert hat.

Demgegenüber ist der Gesetzgebungswille der Vorratsdatenspeicherung in den USA trotz vieler Forderungen nicht erfolgreich, nachdem die Tatsache offenbart wurde, dass in der Vergangenheit in der Praxis die Daten aller Personen ohne Einschränkung und im Geheimen erhoben und gespeichert wurden. Die anlassgebundene Datenspeicherung wird indes weiterhin aufrechterhalten und es wird angestrebt, zum Schutz der Freiheitsrechte des Einzelnen die Datenspeicherung durch den Freedom Act einzuschränken.

Mit der Vorratsdatenspeicherung wurde in Deutschland ein System eingeführt, das dem Überwachungsprogramm der NSA in den USA ähnelt. Dabei werden die Metadaten (jedoch nicht die Daten) der Anrufe, Textnachrichten oder E-Mails aller Bürger für zukünftige Strafverfolgungs- und Terrorismusbekämpfungszwecke erhoben und gespeichert. Die beiden Programme wurden von ähnlichen Bestrebungen inspiriert, die nationalen Sicherheitsbehörden mit wirksamen Instrumenten zur Bekämpfung terroristischer Bedrohungen auszustatten, indem digitale Muster von Interaktionen und Verbindungen zwischen Individuen identifiziert werden.[676]

Ein systematischer und funktionaler Vergleich zwischen der anlasslosen vorrätigen Datenspeicherung und der anlassgebundenen Datenspeicherung ist hinsichtlich der Frage bemerkenswert, ob Schutzlücken durch Wegfall der Vorratsdatenspeicherung entstehen würden, worüber sich

676 *Fabbrini*, Human Rights in the Digital Age: The Europe Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States, Harvard Human Rights Journal, Tilburg Law School Research Paper No. 15, 2014, S. 90.

manche sorgen, oder ob die Vorratsdatenspeicherung im Hinblick auf den Datenschutz schwächer wäre als eine anlassgebundene Datenspeicherung.

b) Aktuelle Rechtslage

Da in Deutschland die Erhebung, Speicherung und Verarbeitung personenbezogener Daten nach dem Bundesdatenschutzgesetz grundsätzlich verboten sind, werden sie durch die Ermächtigungsnormen mit den grundrechtlichen Einschränkungen erlaubt. Dagegen ist der Umgang mit den personenbezogenen Daten in den USA grundsätzlich erlaubt, wo man über fast kein einzelnes Datenschutzgesetz verfügt, weshalb dieser Umgang gesetzlich eingeschränkt wird, was auf den Erfahrungen mit der staatlichen Datenspeicherungspraxis beruht.

Hierbei sind das TKG und die StPO die Ermächtigungsnormen zur Vorratsdatenspeicherung. Mit der Einführung der Vorratsdatenspeicherung werden die Verkehrsdaten, auf die die Ermittlungsbehörden zugreifen dürfen, abgesichert und erweitert. Allgemein wird anerkannt, dass die Erhebung, Speicherung und Verwendung personenbezogener Daten eine Einschränkung der Grundrechte zur Folge haben. Zur Rechtfertigung dieses Grundrechtseingriffs soll verfassungsrechtlich der Grundsatz der Verhältnismäßigkeit betont werden. Der Gesetzgeber musste einerseits die praktische Erforderlichkeit anerkennen, aber andererseits die Eingriffsintensität der anlasslosen vorrätigen Datenspeicherung in Betracht ziehen. Er wollte nach den Anforderungen des Bundesverfassungsgerichts mehrere Datenschutzvorkehrungen gesetzlich bereitstellen und die Eingriffsintensität vermindern. Trotz gesetzgeberischer Datenschutzbemühungen werden weiterhin Einwände gegen die Vorratsdatenspeicherung erhoben.

Bei der US-amerikanischen anlassgebundenen Datenspeicherung wurden umgekehrt einige Gesetze erlassen, damit die Datenspeicherung nicht erlaubt wird, sondern die einschränkungslose Datenspeicherung zum Zweck des Datenschutzes verhindert wird. Die Gesetze zielen darauf ab, die Datenerhebung durch die Ermittlungsbehörden zu erleichtern und zugleich ihre Datenerhebung an bestimmte Voraussetzung zum Datenschutz zu binden. In einem solchen System muss der Erfolg der behördlichen Datenerhebung von der Datenspeicherungspraxis der privaten Telekommunikationsunternehmen abhängen. Die USA wenden dennoch ein solches System an, da die Datenerhebung und -speicherung durch den Diensteanbieter der Telekommunikation wegen eines fehlenden einheitlichen Datenschutzgesetzes abgesehen von bestimmten Bereichen in der Regel

fast nicht eingeschränkt werden kann. Das anlassgebundene Datenspeicherungssystem gewinnt hier eine Wirkungskraft durch das CALEA von 1994,[677] das technische Unterstützung für den Diensteanbieter vorschreibt.

aa) Zu speichernde Daten

In Deutschland stützt sich die Vorratsdatenspeicherung auf die vorrätige Speicherung elektronischer Kommunikationsdaten durch private Diensteanbieter. Die Ermittlungsbehörden kontrollieren die Daten nicht direkt, sondern sie können nur den Zugriff auf diese Daten über private Telekommunikationsanbieter nach gesetzlichen Kriterien beantragen. Im Gegensatz hierzu erhob und speicherte in den USA früher die Regierung selbst die Daten über ihr einst geheimes elektronisches Überwachungsprogramm. Bei den Reformdebatten wurde diskutiert, ob die Datenspeicherung tatsächlich von der NSA auf private Unternehmen verlagert werden sollte.[678] US-Präsident *Obama* veranlasste die Übernahme dieser Aufgabe durch die Diensteanbieter der Telekommunikation. Die Gesetzgebung hat auch in diese Richtung gezeigt, um die Probleme zu lösen, die durch die Überwachung durch die NSA aufgeworfen wurden.[679] Die Diensteanbieter der Telekommunikation speichern die Daten, staatliche Behörden dürfen nach dem ECPA auf diese Daten aber nur zugreifen.

In Deutschland, wo eine Erhebung, Speicherung und Verarbeitung personenbezogener Daten nach dem BDSG grundsätzlich verboten sind, handelt es sich beim TKG um die Ermächtigungsnormen, mit denen die Diensteanbieter die darin genannten Daten speichern und verarbeiten können. Im TKG werden folgerichtig die Daten abschließend aufgezählt, die der Diensteanbieter gewerblich und zusätzlich nach der Vorratsdatenspeicherung speichern darf. Die Vorratsdatenspeicherung erfordert die Speicherung bestimmter Verkehrs- und Standortdaten im Fall der Nutzung mobiler Telefondienste bzw. der mobilen Nutzung öffentlich

677 Pub. L. No. 103-414, 108 Stat. 4279, codified at 47 U. S. C. §§ 1001–1010.

678 *Londras*, Privatized Counter-Terrorism Surveillance: Constitutionalism Undermined, in: Surveillance, Counter-Terrorism and Comparative Constitutionalism. Abingdon, Oxon: Routledge, Routledge research in terrorism and the law, 2013, 59, 73.

679 *Fabbrini*, Human Rights in the Digital Age: The Europe Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States, Harvard Human Rights Journal, Tilburg Law School Research Paper No. 15, 2014, S. 92–93 m. w. N.

zugänglicher Internetzugangsdienste. Hingegen hängt in den USA der Erfolg eines Zugriffs auf die erforderlichen Daten durch eine staatliche Stelle von der Speicherpraxis privater Telekommunikationsunternehmen ab, weil keine gesetzliche Beschränkung bei der Erhebung, Speicherung und Verarbeitung personenbezogener Daten durch sie Anwendung findet. Bei der Datenspeicherung ist der Diensteanbieter gesetzlich nicht gebunden. Während bei der deutschen Vorratsdatenspeicherung eine Speicherung bestimmter Daten aller Bürger anlasslos und vorrätig erfolgt, wird die Aufbewahrung der Daten in den USA durch den *warrant* oder eine gerichtliche Anordnung auf Grundlage eines *probable cause* oder einer bloßen Erklärung des Zusammenhangs mit der laufenden Untersuchung gesichert. Die Sicherung der Datenaufbewahrung ist konsequenterweise anlassgebunden sowie nachträglich und richtet sich gegen bestimmte Verdächtige.

bb) Zugriff auf Daten

Deutschland erwägt die hohe Eingriffsintensität der anlassunabhängigen Datenspeicherung, indem es die Erhebungsvoraussetzungen für die nach § 113b TKG gespeicherten Daten verschärft. In den USA, die über keine Vorratsdatenspeicherung verfügen, sondern eine verpflichtende Datenspeicherung durch den Diensteanbieter vom vorherigen Ersuchen einer staatlichen Behörde abhängig machen, werden diese Daten eher unter erleichterten Voraussetzungen erhoben.

Für die Erhebung vorrätig anlasslos gespeicherter Daten müssen ein Verdacht eines Verbrechenskatalogs, eine strenge Subsidiarität, die besondere Verhältnismäßigkeit und die gerichtliche Anordnung vorausgesetzt werden. Im Gegensatz hierzu erfordern die USA für die Erhebung von Verkehrsdaten nicht einmal eine Einschränkung auf bestimmte Katalogtaten, eine Subsidiarität oder eine Verhältnismäßigkeit. Die Daten dürfen nicht nur durch einen *warrant* erhoben werden, sondern auch durch eine gerichtliche Anordnung, die auf spezifischen und klaren Tatsachen beruht, aus denen ersichtlich ist, dass Grund zu der Annahme besteht, die angeforderten Daten seien für eine laufende strafrechtliche Untersuchung relevant und wesentlich. Bestimmte Verkehrsdaten können sogar mit einer schriftlichen Anfrage oder einer *subpoena* erhoben werden. Diese Voraussetzungen scheinen auch im Vergleich zur Erhebung der nach § 96 des deutschen Telekommunikationsgesetzes gespeicherten Daten sehr locker zu sein. Mit Blick auf die Grundrechtsbeeinträchtigungsgefahr durch die staatliche Verwendung der Telekommunikationsdaten könnte die lockere

Voraussetzung sehr problematisch sein. Das Problem ist noch größer in den USA, wo es keinerlei solche Bestimmungen gibt, im Gegensatz zu Deutschland, wo das Gesetz die zu speichernden Daten klar vorsieht.

Die nach § 113b TKG gespeicherten Daten dürfen außerdem unter dem Zweckbindungsgrundsatz eingeschränkt verwendet und weitergeleitet werden. Der Verwendungszweck der nach § 113b TKG gespeicherten Verkehrsdaten und die Weitergabe dieser Daten an eine andere Behörde sind also im Gesetz deutlich eingeschränkt, während sich die entsprechenden Einschränkungen im US-amerikanischen Recht nicht finden. In den USA werden die Verkehrsdaten nicht im Voraus gespeichert, aber eine Behörde kann unter erleichterten Voraussetzungen eine Vielzahl von Daten von Telekommunikationsunternehmen ohne Einschränkung erheben, sofern die Behörde dies verlangt.

cc) Löschungspflicht

In Deutschland, wo die Speicherung, Verwendung und Verarbeitung personenbezogener Daten mit einigen Ausnahmen grundsätzlich verboten sind, ist die Löschungspflicht der nach der Vorratsdatenspeicherung gespeicherten Daten vorgesehen. Dabei ist die Speicherdauer unterschiedlich je nach der Eingriffsintensität jener Daten bestimmt, die die zuständige Behörde anfragt. In den USA gibt es hingegen für Telekommunikationsunternehmen keine Löschungspflicht, sondern eine Regelung der Speicherungssicherstellung für einen bestimmten Zeitraum. Dabei kommt die unterschiedliche Bedeutung der Daten beim Grundrechtseingriff nicht in Betracht.

In beiden Ländern wird weder eine Löschung noch ein Übermittlungsverbot nach der Datenverwendung gesetzlich gefordert. Während bei der Datenverwendung die USA keine strikte Zweckbegrenzung vorsehen und die Datenübermittlung bloß an bestimmte und klare Fakten gebunden ist, die eine vernünftige Grundlage für die Annahme darstellen, dass die geforderten Daten im Zusammenhang mit einer laufenden Untersuchung stehen, wird bei der deutschen anlasslosen vorrätigen Datenspeicherung keine Löschungsvorschrift nach der Datenverwendung durch eine enge Zweckbegrenzung des § 113c TKG flankiert. Im Vergleich mit den USA werden in Deutschland verschiedene Maßnahmen – die Löschungspflicht nach einem bestimmten Zeitraum, die unterschiedliche Speicherdauer und die enge Zweckbegrenzung bei der Datenverwendung – ergriffen, damit das Risiko einer Verletzung von Grundrechten aufgrund von Daten-

speicherungspraktiken verringert wird. Bedauerlich ist aber weiterhin der trotz dieser grundrechtsschützenden Bemühungen bestehende Mangel an einer Regelung zur Löschung der bereits an die Behörden übermittelten und für den eigentlichen Zweck verwendeten Daten.

dd) Mitteilungspflicht

Eine Kenntnisnahme über eine Maßnahme ist die notwendige Voraussetzung für den Rechtsschutz des Einzelnen. Dieser kann den Schutz gegen eine unbefugte oder übermäßige Erhebung, Speicherung, Verwendung und Verarbeitung seiner personenbezogenen Daten nur beanspruchen, wenn er davon weiß. In diesem Sinn wird in Deutschland die Pflicht der Benachrichtigung an die Beteiligten der betroffenen Telekommunikation gesetzlich sichergestellt – aber es besteht noch die Unterbleibens- oder Zurückstellungsmöglichkeit bei einem überwiegenden öffentlichen Interesse. Dadurch kann der Einzelne seinen Rechtsschutz verwirklichen. Demgegenüber bleibt die US-amerikanische Verkehrsdatenerhebung ein heimlicher Zugriff, weil für die Erhebung von Verkehrsdaten keine Benachrichtigung erforderlich ist. Damit kann der Einzelne von der staatlichen Maßnahme keine Kenntnis nehmen und seinen Rechtsschutz nicht beanspruchen.[680]

680 Das ist in 18 U. S. C.§ 2703 Abs. e ausdrücklich vorgesehen: "No cause of action shall lie in any court against any provider of wire or electronic communication service, its officers, employees, agents, or other specified persons for providing information, facilities, or assistance in accordance with the terms of a court order, warrant, subpoena, statutory authorization, or certification under this chapter."

Teil 5: Schlussbemerkung

A. Datenschutz vor neuen Herausforderungen

Das digitale Zeitalter hat dem Menschen viele Möglichkeiten eröffnet. Was in der Vergangenheit kaum vorstellbar war, ist heute der Regelfall: elektronische Daten, die täglich und überall erstellt werden, finden mannigfaltige Verwendung und Verarbeitung. Die unter modernsten Datenverarbeitungsbedingungen erlangten Informationen sind zumeist bedeutsamer als die originären Daten an sich. Die schnelle Verarbeitungsgeschwindigkeit und die Speicher- und Verknüpfungsmöglichkeiten im Umgang mit elektronischen Daten machen das menschliche Leben einerseits bequem und praktisch; andererseits können sie das freiheitliche Leben der Menschen jedoch auch gefährden. Aufgrund der Aussagekraft dieser Daten können umfassende Bewegungs- und Persönlichkeitsprofile erstellt werden. Durch die Kombination mit anderen Daten nähern wir uns dem gläsernen Bürger. Der Betroffene kann die Richtigkeit und die Verwendung seiner Daten nicht ausreichend kontrollieren. In bisher unbekannter Weise haben sich die Möglichkeiten einer Einsicht- und Einflussnahme erweitert, die auf das Verhalten des Einzelnen durch psychischen Druck öffentlicher Anteilnahme einzuwirken vermögen.[681] Im Rahmen dieser Herausforderungen steht die Freiheit des Einzelnen auf dem Spiel.

Die Krise der Freiheit wird durch soziale Kontrollmechanismen, die auf gesteigerten gesellschaftlichen Sicherheitsbedürfnissen aufgrund permanenter Verunsicherung,[682] Management von Risikoquellen, die sich nicht auf bestimmte Situationen oder bestimmte Personen beziehen, und Techniken des Ausschlusses gefährlicher Personen[683] basieren, immer weiter verschärft. Die Strafrechtspflege steht mit der Einführung neuer technikgestützter Ermittlungsmaßnahmen, die personenbezogene Daten im Strafverfahren verwenden, ebenfalls vor selbigen Problemstellungen. Die Form der Informationsbeschaffung zur Strafverfolgung und zur poli-

681 BVerfGE 65, 1 (42).

682 *Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert, 3. Aufl., S. 38 ff.

683 *Singelnstein/Stolle*, Die Sicherheitsgesellschaft – Soziale Kontrolle im 21. Jahrhundert, 3. Aufl., S. 87 f.

zeirechtlichen Gefahrenabwehr wurde angesichts neuer technischer Möglichkeiten und sicherheitspolitischer Bedürfnisse beständig ausgebaut. Im Namen der Sicherheitsgewährleistung durch effektive strafrechtliche Ermittlungen entstanden einhergehend mit dem Verlust von Freiheit neue Herausforderungen.

Die Freiheit des Einzelnen bedarf unter den heutigen und künftigen Bedingungen der automatischen Datenverarbeitung in besonderem Maße dem Schutz durch wirksame Vorkehrungen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten des Einzelnen. In diesem Zusammenhang ist die Gewährleistung von Datenschutz von großem Interesse und Aufgabe der modernen Gesellschaft. Zur Bewältigung dieser Datenschutzaufgaben wurden und werden sowohl auf nationaler als auch auf internationaler Ebene zahlreiche Anstrengungen unternommen. Der Schutz personenbezogener Daten als Teil der Privatsphäre unter den modernen Datenverarbeitungsbedingungen kann aus der Verfassung, den einfachen Gesetzen als der Konkretisierung der Verfassung oder den gerichtlichen Entscheidungen anhand allgemeiner Prinzipien und Werte abgeleitet werden.[684] Mit der vorliegenden Arbeit wurde insbesondere aufgezeigt, wie der Datenschutz in Deutschland und den USA implementiert wird. Besondere Anknüpfungspunkte lassen sich hier im Verfassungsrecht und in bestimmten Bereichen des Strafregisters, der Rasterfahndung und der Vorratsdatenspeicherung finden. Ferner wurde in der vorliegenden Arbeit beleuchtet, ob der jeweilige Datenschutz als hinreichend bewertet werden kann, um die Freiheit des Einzelnen effektiv gegen eine potenziell unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner Daten unter der heutigen automatisierten Datenverarbeitung zu schützen.

B. Bilanz der Vergleichsergebnisse

Der Schutz personenbezogener Daten setzt grundsätzlich die Befugnis des Einzelnen voraus, selbst über die Preisgabe und Verwendung seiner personenbezogenen Daten zu bestimmen. Konkret bedeutet dies, dass der Einzelne selbst darüber entscheiden kann, ob, wann, wie und in welchem Maße seine Daten veröffentlicht und verwendet werden. Dieses Recht des Einzelnen hat die deutsche Rechtsprechung aus dem allgemeinen Persönlichkeitsrecht aus Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG abgeleitet

684 *Genz*, Datenschutz in Europa und den USA, S. 7.

und konkretisiert. Der Schutz der Daten gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten wurde vom Bundesverfassungsgericht als eine Voraussetzung der freien Persönlichkeitsentfaltung anerkannt.[685] Zum Schutz dieses Rechts stellte das Bundesverfassungsgericht auch konkrete Anforderungen auf: Gesetzesvorbehalt, Normenklarheitsgebot, Verhältnismäßigkeits- sowie Zweckbindungsgrundsatz, verbunden mit der Forderung nach organisatorischen und verfahrensrechtlichen Vorkehrungen. Demgegenüber wurde in den USA der Begriff der *privacy* noch nicht abschließend definiert, und das Recht auf Datenschutz wurde bisher von der Rechtsprechung nur vermutet. Eine feste verfassungsrechtliche Verankerung ist nicht erkennbar. Das entscheidende Kriterium für den Schutz der Privatheit hat sich gemäß der Rechtsprechung vom physischen Betreten eines Raums zur begründeten Erwartung auf *privacy* gewandelt und somit erweitert. Außerdem wird angesichts der fortgeschrittenen technischen Möglichkeiten die Gewöhnlichkeit der eingesetzten Technik im Hinblick auf die subjektive Katz-Prüfung zusätzlich berücksichtigt.

So wird in Deutschland versucht, durch mehrere miteinander verbundene Grundrechte die verschiedenen Aspekte der Privatsphäre und sogar die personenbezogenen Daten als Teil der Privatsphäre zu schützen. Des Weiteren ist der effektive Schutz der Privatsphäre sowie von personenbezogenen Daten gegen neuartige technikgestützte Beeinträchtigungen dadurch möglich, dass der Schutzbereich des allgemeinen Persönlichkeitsrechts möglichst weit interpretiert wird.[686] Zum Schutz personenbezogener Daten tragen mithin die konkreten Anforderungen bei, die auf der Grundlage des Rechts auf informationelle Selbstbestimmung von der Rechtsprechung entwickelt wurden. Darauf basierend werden die Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten durch das BDSG kontrolliert, das wiederum den Umgang mit personenbezogenen Daten grundsätzlich verbietet und nur ausnahmsweise zulässt. Der EuGH befand, dass das Gefühl, überwacht zu werden, das durch das Sammeln umfangreicher Metadaten erzeugt wird, der Privatsphäre abträglich ist und schlug daher vor, dass der Einzelne dann geschützt werden solle, wenn er mit Hilfe neuer technologischer Mittel mit anderen interagiert. Darüber hinaus forderte der EuGH für Eingriffe in die Privatsphäre ein hö-

685 BVerfGE 65, 1 (43).

686 *Weidner-Braun*, Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung – am Beispiel des personenbezogenen Datenverkehrs im www nach deutschem öffentlichen Recht, S. 76.

heres Maß an gerichtlicher Kontrolle im Hinblick auf Erforderlichkeit und Verhältnismäßigkeit, auch wenn diese Eingriffe aus Gründen der nationalen Sicherheit vorgenommen werden.[687] Deutschland schließt sich beim Schutz der Privatsphäre und der Daten dem EuGH an. Der US-amerikanische Supreme Court hatte kürzlich Interesse an ähnlichen Rechtssachen.[688] Mehrere ständig gültige US-Verfassungsgrundsätze wie etwa die *Third-Party-Doctrine* schränken jedoch den Schutz der Privatsphäre und personenbezogener Daten in der digitalen Welt ein.[689] Indem die US-Verfassung für einen engen inneren und speziellen Bereich den Schutz des Privatlebens i. w. S. zumindest vor hoheitlichen Eingriffen garantiert, so wurde zwar der Rahmen festgelegt, der bestimmte Sphären von Privatheit garantiert, jedoch nur geringe Möglichkeiten bietet, einen alle Bereiche des Privatlebens umfassenden Schutz herbeizuführen.[690] Da hier nur einige bestimmte Bereiche nach dem Grundsatz der „grundsätzlichen Zulassung mit einigen Verbotsausnahmen" rechtlich kontrolliert werden und es kein einheitliches Datenschutzgesetz gibt, scheint der Datenschutz in seiner konkreten Ausgestaltung in den USA noch einen langen Weg vor sich zu haben. Dieser Unterschied hinsichtlich der Grundsätze des Datenschutzes hat zu einer Vereinbarung zwischen der EU und dem Handelsministerium (Department of Commerce) der USA, nämlich zu den Grundsätzen des „Safe Harbor", geführt.[691]

---

687 EuGH, Urteil vom 8. April 2014 in den Rechtssachen C-293/12, C-594/12.

688 In der Rechtssache USA gegen Jones stellte der Gerichtshof einstimmig fest, dass die GPS-Überwachung eines Fahrzeugs, das sowohl geografisch als auch zeitlich den Geltungsbereich eines *warrant* überschreitet, eine Durchsuchung gemäß der vierten Änderung darstellt (United States v. Jones, 132 S. Ct. 945 (949)), und mehrere Richter stellten separat das Erfordernis der Geheimhaltung als Vorbedingung für *privacy* in Frage (United States v. Jones, 132 S. Ct. 945 (957)). In der *Kyllo*-Entscheidung erkannte die Richterin Scalia an, dass die Doktrin des vierten Verfassungszusatzes angepasst werden müsse, um die traditionellen Erwartungen an privacy vor der fortgeschrittenen Technologie zu bewahren (Kyllo v. United States, 533 U. S. 27 (33, 34)).

689 *Fabbrini*, Human Rights in the Digital Age: The Europe Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States, Harvard Human Rights Journal, Tilburg Law School Research Paper No. 15, 2014, S. 91.

690 *Genz*, Datenschutz in Europa und den USA, S. 48.

691 Safe Harbor, Kommissionsentscheidung 2000/520/EG: Entscheidung der Kommission vom 26. Juli 2000 gemäß der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates über die Angemessenheit des von den Grundsätzen des „sicheren Hafens" und der diesbezüglichen „Häufig gestellten Fragen" (FAQ) gewährleisteten Schutzes, vorgelegt vom Handelsministerium der USA.

Die Unterschiede im Hinblick auf die verfassungsrechtlichen Grundlagen und die Grundsätze des Datenschutzes in beiden Ländern wirken sich auch auf konkrete einfachgesetzliche Maßnahmen aus. Zunehmend spielen personenbezogene Daten in Strafverfahren eine verfahrensrechtlich bedeutsame Rolle. Je größer die Wertigkeit personenbezogener Daten in Strafverfahren ist, desto wichtiger ist auch deren Schutz. Die Verarbeitung personenbezogener Daten ohne angemessene Schutzmaßnahmen gegen die unbefugte oder übermäßige Erhebung, Speicherung, Verwendung und Weitergabe sollte nicht gerechtfertigt sein. Im Bereich des Strafregisters, dem klassischen Bereich des Schutzes personenbezogener Daten, erkennt Deutschland das öffentliche Interesse an Strafregistern an, berücksichtigt jedoch auch das Interesse der Verurteilten an ihrer Wiedereingliederung in die Gesellschaft und konkretisiert daher die Notwendigkeit des Datenschutzes hinsichtlich der Strafregistrierungen. Im Rahmen der Abwägung beider Interessen wurden Schutzvorkehrungen getroffen, um einen unbefugten oder übermäßigen Zugriff auf die fraglichen Daten zu verhindern. In den USA hingegen scheinen im Bereich des Strafregisters die Verwaltungsinteressen, die sich aus der effektiven Übermittlung nützlicher Daten an die erforderlichen Stellen ergeben, vorrangig zu sein. Der Privatsphären- und Datenschutz scheint hier Berücksichtigung zu finden. Die Bewertung ergibt sich aus der Tatsache, dass in Deutschland die mitteilungspflichtigen Stellen, die ins BZR einzutragenden Inhalte, die Mitteilungs-, Anfrage- sowie Auskunftsmethode und die Datenverwendung und -weitergabe gesetzlich vorgesehen und daher eingeschränkt werden, während in den USA ausschließlich der Austausch zwischen den Einzelstaaten bundesgesetzlich vorgesehen ist und die Erhebung, Speicherung, Verwendung sowie Weitergabe der Strafregistrierungen den Einzelstaaten überlassen bleibt. Hier gibt es zwar die Einschränkung der Verwendungsberechtigten und des Verwendungszweckes, jedoch erschöpft sich ihre Anwendung in den Strafverfahrensdaten ohne Verurteilung. Das Problem verschärft sich insbesondere dann, wenn nicht nur Strafregistrierungen, sondern auch bloße Verhaftungsdaten gespeichert werden. Es scheint hier ein Mangel an angemessenen Schutzvorkehrungen zu bestehen, um den Einzelnen vor der unbefugten oder übermäßigen Erhebung, Speicherung, Verwendung und Weitergabe zu schützen.

Die entsprechende Vergleichseinschätzung gilt auch bei der Rasterfahndung, bei der bestimmte Personengruppen aus öffentlichen oder privaten Datenbanken herausgefiltert werden, damit Hinweise oder Spuren bekannter oder unbekannter Täter gefunden werden können. Im Rahmen des automatischen maschinellen Datenabgleichs werden zwar in beiden

Ländern die Erfassung vergleichbarer Daten nicht ausdrücklich gesetzlich vorgeschrieben, die Datenverwendung wird jedoch an bestimmte Voraussetzungen geknüpft. Die Voraussetzungen werden in der US-amerikanischen Praxis durch „routine use" mehrfach umgangen, sodass der Schutz der Betroffenen eingeschränkt wird, während die Betroffenen beim deutschen Datenabgleich zutreffend durch die Einschränkung auf Katalogtaten und den Richtervorbehalt geschützt werden. Darüber hinaus wird in Deutschland die Datenverwendung für einen anderen als den ursprünglichen Zweck durch die Aufbewahrungs- und Löschungsvorschrift verhindert. Vergleichbare Schutzregelungen sind in den USA nicht angelegt. In Anbetracht dieser Regelungslage lässt sich feststellen, dass in den USA im Vergleich zu Deutschland auch im Rahmen der Rasterfahndung ein geringerer Schutz personenbezogener Daten gewährt wird. Jedoch ist anzumerken, dass der deutsche Richtervorbehalt problematisch ist, um den Einzelnen zu schützen. Insbesondere deshalb, weil die Bedeutung des Richtervorbehalts durch die Möglichkeit der staatsanwaltschaftlichen Eilanordnung bei Gefahr im Verzug abgeschwächt wird. Ebenso scheint das Bedürfnis nach der Eilanordnung bei der Rasterfahndung nicht nachvollziehbar. Das Problem wird insofern verschärft, als das deutsche Recht für die Erkenntnisse, die unter der staatsanwaltschaftlichen Eilanordnung ohne eine nachträgliche gerichtliche Bestätigung gewonnen werden, keine Löschung und auch kein Verwendungsverbot vorsieht.

Abschließend wendet Deutschland bei der Vorratsdatenspeicherung, deren Gültigkeit bisher offenbleibt, das Doppeltürmodell an. Die Anbieter der Telekommunikationsdienste sind dazu verpflichtet, bestimmte Daten anlasslos zu speichern, während versucht wird, der unbefugten oder übermäßigen Erhebung, Speicherung, Verwendung und Weitergabe personenbezogener Daten dadurch zu begegnen, dass die Strafprozessordnung den Zugriff auf diese Daten an enge Voraussetzungen knüpft. Dies ist in Anerkennung der Notwendigkeit der Vorratsdatenspeicherung unter den modernen Datenverarbeitungsbedingungen das Ergebnis des Ausgleichs des Interesses an der effektiven Strafverfolgung einerseits und des Interesses des Einzelnen am Datenschutz andererseits. Die Vorratsdatenspeicherung wird trotz mehrerer Gesetzgebungsversuche in den USA bisher nicht angewendet. Bei dem US-amerikanischen sog. „Quick-Freeze-Verfahren" bezieht sich die Datenspeicherung – anders als bei der Vorratsdatenspeicherung, bei der Telekommunikationsunternehmen die im Gesetz vorgesehenen Daten für einen bestimmten Zeitraum speichern müssen – unter dem ECPA nur auf bestimmte Daten, die von einer Behörde verlangt werden. Das ECPA stellt je nach Art der von den Strafverfolgungsbehörden

angeforderten Daten unterschiedlich strenge Anforderungen. Es ist überraschend, dass die USA, die kein Datenschutzgesetz statuieren, dennoch konkrete Anforderungen an das Quick-Freeze-Verfahren stellen. Angesichts des Umstands, dass in den USA der Umgang mit personenbezogenen Daten im privaten Bereich nicht gesetzlich beschränkt ist, ist es jedoch schwer festzustellen, ob dieses System in den USA dem Schutz personenbezogener Daten zuträglicher ist als die deutsche Vorratsdatenspeicherung.[692]

C. Rechtspolitische Empfehlungen

Ein Interessenausgleich ist eine herausfordernde Aufgabe für den Gesetzgeber, der den verfassungsrechtlichen Konflikt zwischen Freiheit und Sicherheit beilegen muss, indem er das Sicherheitsinstrument auf das notwendige Maß beschränkt und dessen Missbrauchspotenziale soweit wie möglich vermeidet oder vermindert. Angesichts neuer Bedrohungen muss sich die Rechtslehre diesbezüglich weiterentwickeln. Die Möglichkeiten der modernen Datenverarbeitungstechnologie sind enorm. Im digitalen Zeitalter sollten rechtliche Sicherungsmaßnahmen für den Privatsphären- und Datenschutz weiter gestärkt und ausgebaut werden. Denn unter den modernen Datenverarbeitungsbedingungen haben personenbezogene Daten sehr große Aussagekraft. Diesen Daten sind nicht nur vielfältige Auswertungsmöglichkeiten, sondern auch erhebliche Missbrauchspotenziale inhärent, die die Freiheit des Einzelnen gefährden können. Die computergestützte Verarbeitung von Daten führt aufgrund der Verarbeitungsgeschwindigkeit und der Verknüpfungs- und Speichermöglichkeiten zur Gefahr der Entstehung eines umfassenden Überwachungsstaates, die ungleich größer ist als die der manuellen Datenverarbeitung. In der Regulierung der einzelnen Maßnahmen ist somit ein Ausgleich der Interessen von Sicherheit und Freiheit anzustreben und zu erreichen. Unabdingbar ist daher die Auswertung personenbezogener Daten mit angemessenen Schutzvorkehrungen, die den Einzelnen gegen die unbefugte oder übermäßige Erhebung, Speicherung, Verwendung und Weitergabe ihn betreffender Daten hinrei-

692 Dazu kritisch siehe *Ringland*, The European Union's Data Retention Directive and the United States's Data Preservation Laws: Finding the Better Model, 5 Shidler J. L. Com. & Tech. 13, 2009, S. 7: *Ringland* vertritt die Auffassung, dass durch das US-amerikanische Datenspeicherungsmodell im Vergleich zu der deutschen Vorratsdatenspeicherung eine bessere Abwägung zwischen der Unterstützung der Strafverfolgung und der Minimierung der Kosten für Unternehmen und Verbraucher erreicht wird.

chend schützt. Hierfür ist es erforderlich, dass dem Betroffenen bewusst ist, welche seiner personenbezogenen Daten wo, in welchem Umfang und wie genutzt werden. Im Folgenden werden die Empfehlungen an den Gesetzgeber für einen Interessenausgleich bei der Regulierung konkreter Sicherheitsmaßnahmen zusammengefasst:

1. Die Erhebung und Speicherung personenbezogener Daten müssen präzisen vorgesehenen Befugnissen und Voraussetzungen unterliegen. Die im Rahmen aller Ermittlungsmaßnahmen zu verwendenden Daten sind gesetzlich einzuschränken.
2. Bezogen auf Sensitivität und Vulnerabilität sind verschiedene Datenkategorien zu unterscheiden, die wiederum differenzierten Speicherfristen, Verwendungsbefugnissen und Schutzvorkehrungen unterliegen.
3. Die Datenverwendung ist an einen bestimmten Verwendungszweck zu binden, um dem Risiko der unbegrenzten Verwendung auch für andere Zwecke als den ursprünglichen zu begegnen.
4. Der Umgang mit personenbezogenen Daten ist den Betroffenen durch eine Benachrichtigung mitzuteilen, sodass dieser eine Kontrollmöglichkeit erhält. Die Benachrichtigung der Betroffenen garantiert Rechtsschutz. Der effektive Schutz des Rechts auf informationelle Selbstbestimmung setzt voraus, dass die Bürger grundsätzlich Kenntnis davon haben müssen, über welche sie betreffenden Daten staatliche Stellen verfügen.
5. Die Zulässigkeit konkreter Maßnahmen ist von Gerichten zu überprüfen. In diesem Zusammenhang ist die Möglichkeit der staatsanwaltschaftlichen Eilanordnung bei der Rasterfahndung zu streichen.

Literaturverzeichnis

Ahuja, M. FAQ: What you need to know about NSA surveillance and Edward Snowden, WASHINGTON POST v. 5.8.2013, abrufbar unter: https://www.propublica.org/article/nsa-data-collection-faq.

Albrecht, H.-J. Der erweiterte Sicherheitsbegriff und seine Folgen, RAV Infobrief # 91. 2003.

– Schutzlücken durch Wegfall der Vorratsdatenspeicherung - Eine Untersuchung zu Problemen der Gefahrenabwehr und Strafverfolgung bei Fehlen gespeicherter Telekommunikationsverkehrsdaten. Gutachten des Max-Planck-Instituts für ausländisches und internationales Strafrecht, im Auftrag des Bundesministerium der Justiz, 2011.

– Sicherheit und Prävention in strafrechtlichen Sanktionensystemen: Eine kriminologische, komparative Untersuchung. in: H.-G. Koch, Wegsperren? - Freiheitsentziehende Maßnahmen gegen gefährliche, strafrechtlich verantwortliche (Rückfall-)Täter. Berlin, 2011.

Albrecht, P.-A. *Jugendstrafrecht, 3. Aufl.* München, 2000.

– Kriminologie, 4. Aufl. München, 2010.

– Vom Präventionsstaat zur Sicherheitsgesellschaft, Wege kontinuierlicher Erosion des Rechts, in: Herzog F./Hassemer W. (Hrsg.) Festschrift für Winfried Hassemer. Heidelberg, 2010, 3.

Azarchs, T. *Informational Privacy: Lessons from Across the Atlantic, 16 U. Pa. J. Const. L. 805, 2014 .*

Backes, O./Gusy, C. *Wer kontrolliert die Telefonüberwachung? - Eine empirische Untersuchung zum Richtervorbehalt bei der Telefonüberwachung.* 2003.

Baker, J. E. *In the Common Defense.* Cambridge Uni. Press, 2009.

Bär, W. „Anmerkung zum Urteil des BVerfG: Verfassungsmäßigkeit der Online-Durchsuchung und anderer verdeckter Ermittlungsmaßnahmen in Datennetzen, MMR 2008, 325."

– Beck'scher Onlinekommentar zur StPO, § 100g (zitiert nach Bär, BeckOK-StPO, § 100g.

– Beck'scher Onlinekommentar zur TKG, § 113b (zitiert nach Bär, BeckOK-TKG, § 113b.

– Handbuch zur EDV-Beweissicherung im Strafverfahren, 2007.

– TK-Überwachung, §§ 100a - 101 StPO mit Nebengesetzen Kommentar, 2010.

Barnett, R. *Why the NSA Data Seizures are unconstitutional, Harvard Journal of Law & Public Policy, Vol. 38 No. 1.* 2014.

Behr, J. *Vollstreckung ohne Durchsuchungsanordnung, NJW 1992, 2125.*

Bludovsky, O. *Rechtliche Probleme bei der Beweiserhebung und Beweisverwertung im Zusammenhang mit dem Lauschangriff nach § 100 c Abs. 1 Nr. 3 StPO.* Frankfurt a. M., 2002.

Böckenförde, E.-W. *Grundrechtstheorie und Grundrechtsinterpretation, in: ders., Staat, Gesellschaft, Freiheit. Studien zur Staatstheorie und zum Verfassungsrecht, Frankfurt a. M., 1976.*

Brin, D. *The Transparent Society, 1998.*

Bruns, M. *in: Hannich, R. (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung mit GVG, EGGVG und EMRK, 8. Aufl., § 100a,.* München, 2019.

Brunst, P. W. *Anonymität im Internet - rechtliche und tatsächliche Rahmenbedingungen.* Freiburg, 2009.

Bull, H. P. *Datenschutz oder die Angst vor dem Computer.* München, 1984.
– *Informationelle Selbstbestimmung - Vision oder Illusion?: Datenschutz im Spannungsverhältnis von Freiheit und Sicherheit, 2. Aufl.* Tübingen, 2011.

Büllingen, F. *Vorratsdatenspeicherung von Telekommunikationsdaten im internationalen Vergleich, DuD 2005, 349.*

Bundestag, Der Deutsche. *Plenarprotokoll 16/19, Stenographischer Bericht, 19. Sitzung in der 16. Wahlperiode, Berlin, 16.2.2006, abrufbar unter:* http://dip.bundestag.de/btp/16/16019.pdf.

de Busser, E. *Data Protection in EU und USA Criminal Cooperation: A Substantive Law Approach to the EU Internal and Transatlantic Cooperation in Criminal Matters Between Judicial and Law Enforcement Authorities.* 2009.

Carlson, S. C./Miller, E. D. *Public Data and Personal Privacy, Santa Clara High Technology Law Journal, Vol. 16 Issue 1, 2000, abrufbar unter:* https://digitalcommons.law.scu.edu/chtlj/vol16/iss1/4/.

Center for Democracy and Technology. *Introduction to Data Retention Mandates, 2012, abrufbar unter:* https://cdt.org/wp-content/uploads/pdfs/CDT_Data_Retention-Five_Pager.pdf.

Chmielewski, M. *Die Vorratsdatenspeicherungsrichtlinie und ihre Umsetzung in Deutschland und in Polen.* Hamburg, 2013.

Clarke, R. A. *A Normative Regulatory Framework for Computer Matching, Vol. 13 Issue 4, Journal of Computer & Information Law, 1995, abrufbar unter:* https://repository.jmls.edu/cgi/viewcontent.cgi?article=1363&context=jitpl.
– *Computer Matching and Digital Identity, abrufbar unter:* http://www.rogerclarke.com/DV/CFP93.html. San Francisco, 1993.
– *Dataveillance by Governments: The Technique of Computer Matching, Information Technology & People, Vol. 7 No. 2, 1994, 46.*

Comans, C. D. *Ein "modernes" europäisches Datenschutzrecht - Bestandsaufnahme und Analyse praktischer Probleme des europäischen Datenschutzes unter besonderer Berücksichtigung der Richtlinie zur Vorratsdatenspeicherung.* Frankfurt am Main, 2012.

Cooley, T. M. *A Treatise on the Law of Torts or the Wrongs Which Arise Independent of Contract, 2nd ed.* Chicago, 1888.

Crump, C. *Data Retention: Privacy, Anonymity, and Accountability Online, Stanford Law Review, Vol. 56, p. 191.* 2003.

Dalby, J. *Vorratsdatenspeicherung - Endlich?!, KriPoZ 2016, 113.*

Degenhart, C. *Das allgemeine Persönlichkeitsrecht, Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 GG, JuS 1992, 362.*

Derksen, R. *Unionsrechtskonforme Spielräume für anlasslose Speicherung von Verkehrsdaten?, NVwZ 2017, 1005.*

Diehm, J. W. „Federal Expungement: A Concept in Need of a Defination, St. John's Law Review, Vol 66. No. 1, 1992, 73, abrufbar unter: https://scholarship.law.stjohns.edu/cgi/viewcontent.cgi?article=1758&context=lawreview."

Dix, A. *Freiheit braucht Sicherheit - Sicherheit braucht Freiheit, Benjamin Franklin und die Freiheit zur unbeobachteten Kommunikation, in: Bundeskriminalamt (Hrsg.), Informations- und Kommunikationskriminalität, .* Vorträge anlässlich der Herbsttagung des Bundeskriminalamtes vom 2. bis 4. Dezember 2003, München 2004,

Ehmann, H. *Zur Struktur des Allgemeinen Persönlichkeitsrechts, JuS 1997, 193.*

Eifert, M. *Informationelle Selbstbestimmung im Internet, NVwZ 2008, 521.*

Epping, V. *Grundrechte, 8 Aufl.* ORT? 2019.
– *Grundrechte, 8. Aufl.* Berlin, 2019.

Erb, V. *in: Löwe-Rosenberg (Hrsg.), Die Strafprozessordnung und das Gerichtsverfassungsgesetz: Großkommentar, 27. Aufl., § 163d.* Berlin/Boston, 2018.

Ermisch, G. *Fahndung und Datenschutz - aus der Sicht der Polizei, in: Bundeskriminalamt (Hrsg.), Möglichkeiten und Grenzen der Fahndung, Vortragsreihe Bd. 25.* Wiesbaden, 1980.

Fabbrini, F. *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States, Harvard Human Rights Journal, Tilburg Law School Research Paper No. 15, 2014.*

Fan, M. D. *Constitutionalizing Informational Privacy by Assupmtion, 14 U. Pa. J. Const. L. 953, 2012.*

Fos, D. *Der IMSI-Catcher, DuD 2002, 212.*

Geis, M.-E. *Großer Aufwand für großen Lauschangriff, JuS 1998, 1174.*

Gemählich, R. *in: Heintschel-Heinegg/Bockemühl (Hrsg.), Kommentar zur Strafprozessordnung, § 493 (zitiert nach Gemählich, KMR, § 493).* 2011.

Genz, A. *Datenschutz in Europa und den USA, 1. Aufl.* Wiesbaden, 2004.

Gercke, B. *in: Gercke, B./Julius, K.-P./Temming, D./Zöller, M. A. (Hrsg.), Heidelberger Kommentar zur Strafprozessordnung, 6 Aufl., ORT? 2019.*
– in: Gercke, B./Julius, K.-P./Temming, D./Zöller, M. A. (Hrsg.), Heidelberger Kommentar zur Strafprozessordnung, § 100f, 6. Aufl. Heidelberg, 2019.

Gercke, M. *Heimliche Online-Durchsuchung: Anspruch und Wirklichkeit, CR 2007, 245.*

Germann, M. *Gefahrenabwehr und Strafverfolgung im Internet.* Berlin, 2000.

Gieg, G. *in: Hannich, R. (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung mit GVG, EGGVG und EMRK, 8. Aufl., §§ 474, 489 und 494.* München, 2019.

Glauben, P. J. *Kann der „Große Lauschangriff" zulässig sein? Ein Überblick über die verfassungsrechtlichen Aspekte, DRiZ 1993, 41.*

Götz, A. *Das Bundeszentralregister, 3. Aufl.* Köln, 1985.

Götz, V. *Allgemeines Polizei- und Ordnungsrecht, 12. Aufl., 1995.*

Gray, D./Citron, D. K. *A Shattered Looking Glas: The Pitfalls and Potential of the Mosaic Theory of Fourth Amendment Privacy, North Carolina Journal of Law and Technology, Vol. 14, No. 2, 2013, 381.*

Greenwald, G. *No Place to Hide: Edward Snowden, the NSA, and the U. S. Surveillance State.* Metropolitan Books, 2015.

Greven, M. *in: Hannich, R. (Hrsg.), Karlsruher Kommentar zur Strafprozessordnung mit GVG, EGGVG und EMRK, 8. Aufl., § 98a und § 98b.* München, 2019.

Grimm, D. *Aus der Balance, Die Zeit v. 28.11.2007, abrufbar unter:* https://www.zeit.de/2007/49/Schaeuble-Antwort.

Groenemeyer, A. *Wege der Sicherheitsgesellschaft, Gesellschaftliche Transportionen der Konstruktion und Regulierung innerer Unsicherheiten.* Heidelberg, 2010.

Gropp, W. *Rechtsvergleicher Querschnitt, in: Besondere Ermittlungsmaßnahmen zur Bekämpfung der Organisierten Kriminalität, 815 .* Freiburg, 1993.

Guttenberg, U. *Die heimliche Überwachung von Wohnungen – Zur verfassungsrechtlichen Problematik des § 9 II, III BVerfSchG und verwandter Vorschriften, NJW 1993, 567.*

Hauck, P. *in: Löwe-Rosenberg (Hrsg.), Die Strafprozessordnung und das Gerichtsverfassungsgesetz: Großkommentar, 27. Aufl., §§ 100a und 100g.* Berlin/Boston, 2019.

Hellmann, U. *in: Wassermann, R. (Hrsg.), Kommentar zur Strafprozessordnung in der Reihe Alternativ-Kommentare, Bd. 3, .ORT?* 1996.

Hermes, G. *in: Dreier, H. (Hrsg.), Grundgesetz, 3. Aulf., Band I, Art. 10 und 13.* Tübingen, 2013.

Herrmann. *in: Hanns Seidel Stiftung (Hrsg.) Politische Studien Bd. 458 (Im Fokus) 14.*

Herrmann, J. *Vorratsdatenspeicherung ist notwendig, in: Hanns Seidel Stiftung (Hrsg.), Politische Studien Bd. 458 im Fokus „Frei oder Sicher? – brauchen wir die Vorratsdatenspeicherung? 14.*

Hilger, H. *Gesetzgebungsbericht - §§ 100g, 100h StPO, die Nachfolgeregelungen zu § 12 FAG, GA 2002, 228.*
– Gesetzgebungsbericht: Über den neuen § 100i StPO, GA 2002, 557.
– in: Löwe-Rosenberg (Hrsg.), Die Strafprozessordnung und das Gerichtsverfassungsgesetz: Großkommentar, 26. Aufl., § 492. Berlin/New York, 2010.

Hirsch, B. *Gesellschaftliche Folgen staatlicher Überwachung, DUD 2008, 87.*

Hoffmann, M. „Die Online-Durchsuchung: staatliches Hacken oder zulässige Ermittlungsmaßnahme?", NStZ 2005, 121.

Hoffmann-Riem, W. *Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme, JZ 2008, 1009.*

Holland, M. *Bundesnetzagentur setzt Vorratsdatenspeicherung aus, heise online v. 28.6.2017, abrufbar unter* https://www.heise.de/-3757527.html.

Hömig, D. *"Neues" Grundrecht, neue Fragen?, Zum Urteil des BVerfG zur Online-Durchsuchung, Jura 2009, 207.*

Horn, H.-D. *in: Stern, K./Becker, F., Grundrechte-Kommentar, 2. Aufl., 2016, Art. 2.*

Hornig, J. C. *Sicherheit statt Freiheit.* ORT? 2010.

Hu, M. *Bulk Biometric Metadata Collection, North Carolina Law Review, Vol. 96.* 2018.

Huster, S./Rudolph, K. *Vom Rechtsstaat zum Präventionsstaat.* Frankfurt am Main, 2008.

Isensee, J. *Das Grundrecht auf Sicherheit.* Berlin, 1983.

Jacobs, J. B./Blitsa, D. *Sharing Criminal Records: The United States, the European Union and Interpol Compared, 30 Loy. L.A. Int'l & Comp. L. Rev. 125 (2008) /Loyola of Los Angeles International and Comparative Law Review, Vol. 30, Issue 2 (Spring 2008), 125.*

Jacobs, J./Crepet, T. *The Expanding Scope, Use and Availability of Criminal Records, Legislation and Public Policy, Vol 11: 177.* 2008.

Jakobs, J. B. *Mass Incarceration and the Proliferation of Criminal Records, Vol. 3 Issue 3.* Univ. Of St. Thomas Law Journal, 2006.

Jarass, H. D. *in: ders./Pieroth (Hrsg.), Grundgesetz für die Bundesrepublik Deutschland, 15. Aufl.* München, 2018.

Jehle, J.-M./Heinz, W./Sutterer, P. *Legalbewährung nach strafrechtlichen Sanktionen. Eine kommentierte Rückfallstatistik.* Berlin, 2003.

Justice, U. S. Department of. *Compendium of State Privacy and Security Legislation: 2002 Overview, BUREAU OF JUSTICE STATISTICS, 2003.*

Justice, U. S. Department of. "Report of the National Task Force on Privacy, Technology, and Criminal Justice Information", 2001, Bureau of Justice Statistics, abrufbar unter: https://www.bjs.gov/content/pub/pdf/rntfptcj.pdf.

Kadidal, S. *NSA Surveillance: The Implications For Civil Liberties, abrufbar unter:* https://de.scribd.com/document/195673468/NSA-Surveillance-The-Implications-for-Civil-Liberties-Kadidal. 2014.

Kalf, W. *Die Fristen des Bundeszentralregistergesetzes in der strafrechtlichen Praxis, StV 1991, 137.*

Kestel, O. *§§ 474 ff. StPO - eine unbekannte Größe, StV 1997, 266.*

Kingreen, T./Poscher, R. *Grundrechte Staatsrecht II, 34. Aufl., 2018, Heidelberg.*

Krempl, S. *34,443 Klageschriften gegen die Vorratsdatenspeicherung, heise online v. 29.2.2008, abrufbar unter:* http://www.heise.de/-185285.html.

Kuhn, M. *Federal Dataveillance: Implications for Constitutional Privacy Protections.* New York, 2007.

Kühne, J.-D. *in: Sachs (Hrsg.), Grundgesetz, 8. Aufl., 2018, München, Art. 13.*

Kunig, P. *Grundgesetz-Kommentar, 6. Aufl., 2012, München.*

Kutscha, M. *in: Roggan/Kutscha (Hrsg.), Handbuch zum Recht der Inneren Sicherheit, 2. Aufl., 2006, Berlin.*

Laudon, K. C. *Computers and Bureaucratic Reform.* Wiley, 1974.

Legnaro, A. *Konturen der Sicherheitsgesellschaft: Eine polemischfuturologische Skizze, In: Leviathan.* 1997.

Lepsius, O. *Das Computer-Grundrecht: Herleitung - Funktion - Überzeugungskraft, in: Roggan, F. (Hrsg.), Online-Durchsuchung - Rechtliche und tatsächliche Konsequenzen des BVerfG-Urteils vom 27. Februar, 2008.* Berlin, 2008, 21.

Leutheusser-Schnarrenberger, S. *Die Beerdigung 1. Klasse der anlasslosen Vorratsdatenspeicherung in Europa, DuD 2014, 589.*

Levenshtein, R. *Vorratsdatenspeicherung auf Eis gelegt, industr.com v. 29.6.2017, abrufbar unter* https://www.industr.com/-2296251.

Linowes, D. F. *Privacy in America: Is Your Private Life in the Public Eye? Urbana [u. a.], Univ. of Illinois Press, 1989.*

Londras, F. *Privatized Counter-Terrorism Surveillance: Constitutionalism Undermined, in: Surveillance, counter-terrorism and comparative constitutionalism. Abingdon, Oxon: Routledge, Routledge research in terrorism and the law, 2013, 59.* abrufbar unter: http://dro.dur.ac.uk/10795/1/10795.pdf?DDD19+rcfv53+dul4eg,

Lützner, A. *USA, in: Gropp, W. (Hrsg.), Besondere Ermittlungsmaßnahmen zur Bekämpfung der Organisierten Kriminalität.* Freiburg, 1993.

Martinson, R. *What works? - questions and answers about prison reform, The Public Interest Issue 35, 22.* 1974.

McAdoo, L. *Creating an Expungement Statute for the District of Columbia: a Report and Proposed Legislation.* Washington, 2006.

McCullagh, D. *Gonzales Pressures ISPs on Data Retention, ZDNET News v. 27.5.2006, abrufbar unter:* https://www.zdnet.com/article/gonzales-pressures-isps-on-data-retention/.

Meyer-Goßner/Schmitt. *Strafprozessordnung, 59. Aufl.* München, 2016.

Moniodis, C. P. *Moving from Nixon to NASA: Privacy's second Strand – A Right to Informational Privacy, 15 YALE J. L. & Tech. 139, 2012.*

Moser-Knierim, A. *Vorratsdatenspeicherung.* Wiesbaden, 2014.

Mukherji, R. „In Search of Redemption: Expungement of Federal Criminal Records, 2013, abrufbar unter: https://scholarship.shu.edu/cgi/viewcontent.cgi?article=1163&context=student_scholarship."

Müller, M. *Der sogenannte „Große Lauschangriff", Eine Untersuchung zu den Rechtsproblemen der Einführung der elektronischen Wohnraumüberwachung zur Beweismittelgewinnung.* Marburg, 2000.

Murswiek, D./Rixen, S. *in: Sachs (Hrsg.), Grundgesetz, 8. Aufl., 2018, München, Art. 2.*

Olivito, J. *Beyond the Fourth Amendment: Limiting Drone Surveillance Through the Constitutional Right to Informational Privacy, Ohio State Law Journal, vol. 74, no. 4 669, 2013 .*

Orantek, K. *Die Vorratsdatenspeicherung in Deutschland, NJ 2010, 193.*

Paa, B. *Der Zugriff der Strafverfolgungsbehörden auf das Private im Kampf gegen schwere Kriminalität.* Heidelberg, 2013.

Pagenkopf, M. *in: Sachs (Hrsg.), Grundgesetz, 8. Aufl., 2018, München, Art. 10.*

Pager, D. *The Mark of a Criminal Record, American Journal of Sociology 108 (5):937.*

Petersen, R. *Toward a U. S. Data-Retention Standard for ISPs, EDUCAUSE Review, Vol. 41, No. 6, 2006, 78-79.*

Plath, K.-U. *in: Plath (Hrsg.), DSGVO/BDSG Kommentar, 3. Aufl.* Köln, 2018.

Rebmann, K. *Einhundert Jahre Strafregisterwesen in Deutschland, NJW 1983, 1513.*

Rebmann, K./Uhlig, S. *Bundeszentralregistergesetz.* München, 1985.

Reid, M. M. *NSA and DEA Intelligence Sharing: Why it is legal and why REUTERS and the GOOD WIFE got it wrong, SMU Law Review, Vol. 68 Issue 2, abrufbar unter:* http://scholar.smu.edu/cgi/viewcontent.cgi?article=1029&context=smulr. 2015.

REPORT, The 9/11 COMMISSION. *abrufbar unter:* https://www.govinfo.gov/content/pkg/GPO-911REPORT/pdf/GPO-911REPORT.pdf.

Riegel, R. *Rechtsprobleme der Rasterfahndung, ZRP 1980, 300.*

Ringland, K. *The European Union's Data Retention Directive and the United States's Data Preservation Laws: Finding the Better Model, 5 Shidler J. L. Com. & Tech. 13, 2009.* abrufbar unter: http://digital.law.washington.edu/dspace-law/bitstream/handle/1773.1/427/vol5_no3_art13.pdf?sequence=1.

Rogall, K. *Moderne Fahndungsmethoden im Lichte eines gewandelten Grundrechtsverständnisses, GA 1985, 1.*

Ronellenfitsch, M. *Datennotwehr, DuD 2008, 110.*

Roßnagel, A. *Die neue Vorratsdatenspeicherung - der nächste Schritt im Ringen um Sicherheit und Grundrechtsschutz, NJW 2016, 533.*

Roßnagel, A./Moser-Knierim, A./Schweda, S. *Interessenausgleich im Rahmen der Vorratsdatenspeicherung.* Baden-Baden, 2013.

Ruthig, J. *Die Unverletzlichkeit der Wohnung (Art. 13 GG n. F.), JuS 1998, 506.*

Sawade, U./Schomburg, W. *Ausgewählte Probleme des Bundeszentralregistergesetzes, NJW 1982, 551.*

Schlegel, S. *Warum die Festplatte keine Wohnung ist - Art. 13 GG und die "Online-Durchsuchung", GA 2007, 648.*

Schmidt, W. *Die bedrohte Entscheidungsfreiheit, JZ 1974, 241.*

Schmitt, B. *in: Meyer-Goßner/Schmitt, Strafprozessordnung, 61. Aufl., 2018, München (zitiert nach Schmitt, Strafprozessordnung, § 100g).*

Schnarr, K. H. *Zur Verknüpfung von Richtervorbehalt, staatsanwaltlicher Eilanordnung und richterlicher Bestätigung, NStZ 1991, 209.*

Schneider, F. *Rechtliche Rahmenbedingungen für die Vornahme von Online-Durchsuchungen,.* Frankfurt am Main, 2012.

Schwartz, P. M. *Zur Architektonik des Datenschutzes in den USA, in: Stern, K./Pfeifer, K.-N./Hain, K.-E., Datenschutz im digitalen Zeitalter.* München, 2015.

Shiffman, J./Cooke, K. *Exclusive: U. S. directs agents to cover up program used to investigate Americans, REUTERS v. 5.8.2013, abrufbar unter:* https://www.reuters.com/article/us-dea-sod/exclusive-u-s-directs-agents-to-cover-up-program-used-to-investigate-americans-idUSBRE97409R.

Sieber, U. *Legitimation und Grenzen von Gefährdungsdelikten im Vorfeld terroristischer Gewalt – Eine Analyse der Vorfeldtatbestände im "Entwurf eines Gesetzes zur Verfolgung der Vorbereitung von schweren staatsgefährdenden Gewalttaten."*, *NStZ 29, 353* . 2009.
– Strafrechtsvergleichung im Wandel: Aufgaben, Methoden und Theorieansätze der vergleichenden Strafrechtswissenschaft, in: Sieber/Albrecht (Hrsg.), Strafrecht und Kriminologie unter einem Dach, Berlin 2006, S. 112 f.

Siebrasse, P. *Strafregistrierung und Grundgesetz - Zur Verfassungsmäßigkeit der Straf(verfahrens)registrierung in BZRG, StPO, BKAG und BGSG.* Frankfurt am Main, 2002.

Siebrecht, M. *Rasterfahndung - Eine EDV-gestützte Massenfahndungsmethode im Spannungsfeld zwischen einer effektiven Strafverfolgung und dem Recht auf informationelle Selbstbestimmung.* Berlin, 1997.
– Rechtsprobleme der Rasterfahndung, CR 1996, 545..

Simitis, S. *Die informationelle Selbstbestimmung - Grundbedingung einer verfassungskonformen Informationsordnung, NJW 1984, 398.*

Singelnstein, T. *Möglichkeiten und Grenzen neuerer strafprozessualer Ermittlungsmaßnahmen - Telekommunikation, Web 2.0, Datenbeschlagnahme, polizeiliche Datenverarbeitung & Co., NStZ 2012, 593.*

Singelnstein, T./Stolle, P. *Die Sicherheitsgesellschaft - Soziale Kontrolle im 21. Jahrhundert.*

Singelnstein, T. *Verhältnismäßigkeitsanforderungen für strafprozessuale Ermittlungsmaßnahmen - am Beispiel der neueren Praxis der Funkzellenabfrage, JZ 2012, 601.*

Solove, D. J./Rotenberg, M./Schwartz, P. M. *Information Privacy Law, 2ed Ed. Aspen, 2005.*

Solove, D. J./Schwartz, P. M. *PRIVACY LAW: FUNDAMENTALS.* Portsmouth, 2011.

Solove, Daniel J./Schwartz, Paul M. *Information Privacy Law, 3. ed.* New York, 2009.

Spiegel, Der. *Verbrechen: Schrei der Hilflosigkeit, Der Spiegel 40/1996 v. 30.9.1996, abrufbar unter:* https://www.spiegel.de/spiegel/print/d-9095363.html.

Steinhauer, J./Weisman, J. *U. S. Surveillance in Place Since 9/11 Is Sharply Limited, The New York Times v. 2.6.2015, abrufbar unter:* https://www.nytimes.com/2015/06/03/us/politics/senate-surveillance-bill-passes-hurdle-but-showdown-looms.html.

Steinmüller, W. *Grundfragen des Datenschutzes: Gutachten im Auftrag des Bundesministeriums des Innern, Deutscher Bundestag – 6. Wahlperiode – BT-Drs. 6/3826 Anlage I.* 1971.

Stolle, P. *Das Strafrecht, seine Zwecke und seine Alternativen, In: Studentische Zeitschrift für Rechtswissenschaft, 27.* 2006.

Swartz, J./Johnson, K. *U. S. asks Internet Firms to Save Data, NEWSWATCH v. 1.6.2006, abrufbar unter:* https://newswatch.write2kill.in/news/2006/06/01/us-asks-internet-firms-to-save-data.

Temming, D./Schmidt, E. C. *in: Gercke, B./Julius, K.-P./Temming, D./Zöller, M. A. (Hrsg.), Heidelberger Kommentar zur Strafprozessordnung, § 100f, 6 Aufl.* Heidelberg, 2019.

Tinnefeld, M.-T. *in: Tinnefeld, M.-T./Buchner, B./Petri, T./Hof, H.-J. (Hrsg.), Einführung in das Datenschutzrecht, 6 Aufl.* Berlin, 2018.

Tolzmann, G. *Bundeszentralregistergesetz, 5. Aufl.* Stuttgart, 2015.

Trojanow, I./Zeh, J. *Angriff auf die Freiheit: Sicherheitswahn, Überwachungsstaat und der Abbau bürgerlicher Rechte.* München, 2010.

U. S. Department of Health, Education & Welfare. *Records, Computers, and the Rights of Citizens: Report of the Secretary´s Advisory Committee on Automated Personal Data Systems.* 1973.

U. S. Department of Justice. „Attorney General´s Report on Criminal History Background Checks, 2006, abrufbar unter: https://www.bjs.gov/content/pub/pdf/ag_bgchecks_report.pdf."

U. S. Department of Justice. „Survey of State Criminal History Information Systems, 2003, Bureau of Justice Statistics, abrufbar unter: https://www.bjs.gov/content/pub/pdf/sschis03.pdf."

U. S. Department of Justice. „Use and Management of Criminal History Record Information: A Comprehensive Report, 2001 Update, Bureau of Justice Statistics, abrufbar unter: https://www.bjs.gov/content/pub/pdf/umchri01.pdf."

Warren, S./Brandeis, L. *The Right to Privacy, Harvard Law Review, Vol. 4, No. 5., 1890, 193, abrufbar unter:* https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf.

Weichert, T. *Grundrechte in der Informationsgesellschaft, DuD 2000, 104.*

Weidner-Braun, Ruth. *Der Schutz der Privatsphäre und des Rechts auf informationelle Selbstbestimmung - am Beispiel des personenbezogenen Datenverkehrs im www nach deutschem öffentlichen Recht.* Berlin, 2012.

Wiedemann, G. *Regieren mit Datenschutz und Überwachung.* Marburg, 2011.

Wohlers, W./Demko, D. *Der strafprozessuale Zugriff auf Verbindungsdaten (§§ 100g, 100h StPO), StV 2003, 241.*

Wolter, J. *Datenschutz und Strafprozeß, ZStW 1995, 793.*

Young, J. M. *Surfing While Muslim: Privacy, Freedom of Expression & the Unintended Consequences of Cybercrime Legislation, International Journal of Communications Law & Policy, No. 9, 2004.*

Zimmer, H. *Zugriff auf Internetzugangsdaten: Unter besonderer Berücksichtigung der Verhältnismäßigkeit einer verdachtsunabhängigen Vorratsdatenspeicherung, 2012.*

Zippelius, R./Würtenberger, T. *Deutsches Staatsrecht, 33. Aufl.* 2018.